Ein generisches Intrusion Prevention System mit dynamischer Bandbreitenbeschränkung

Detlef Fliegl, Timo Baur, Helmut Reiser, Bernhard Schmidt
Leibniz Rechenzentrum der Bayerischen Akademie der Wissenschaften, LRZ [2]
fliegl|timo.baur|reiser|schmidt@lrz.de

Abstract:
Metropolitan Area Networks wie das Münchner Wissenschaftsnetz (MWN) bieten aufgrund ihrer Größe viele Missbrauchsmöglichkeiten von aussen und zunehmend auch von innen. So stellen beispielsweise durch Würmer und Viren verseuchte Systeme längst keine Einzelfälle mehr dar. Regelmässig kommt es dadurch zu Beschwerden anderer Nutzer und auch zu Beeinträchtigungen von ganzen Netzbereichen. Zudem lassen sich die meisten infizierten Rechner durch sog. Bot-Netz Kommandos komplett fernsteuern oder ausspähen. In Folge fällt auf der Administrationsseite durch die manuelle Reaktion und Bearbeitung solcher Problemfälle ein erheblicher Aufwand an. Um diesen Bearbeitungsaufwand zu verringern, gleichzeitig aber das Sicherheitsniveau zu erhöhen, wurde am Leibniz–Rechenzentrum (LRZ) ein generisches Intrusion Prevention System (IPS) entwickelt. Dieses System — Nat-O-Mat — realisiert ein statistisches und signaturbasiertes Intrusion Prevention System mit einer feingranularen Verwaltung von Policies. Darüber hinaus können bei Verstößen gegen die festgelegten Policies nach einem Eskalationsprinzip automatisch unterschiedliche Maßnahmen ergriffen werden. Auch kann die Bandbreite für beliebige Protokollklassen, wie z.B. P2P-Verkehr, dynamisch beschränkt werden, ohne den restlichen Verkehr zu behindern. Das System hat sich im Einsatz hervorragend bewährt und führte auf Administratorenseite zu deutlichen Erleichterungen im Betrieb des Netzes bei gleichzeitig positiver Resonanz auf Seiten der Nutzer.

1 Motivation

Im Münchner Wissenschaftsnetz (MWN) werden mehr als 50.000 IP-Endsysteme betrieben [8]. Neben einer geringen Anzahl von Servern handelt es sich dabei hauptsächlich um Arbeitsplatzrechner oder Notebooks. Dabei werden nicht alle Systeme von individuellen Firewalls und Antiviren-Programmen geschützt, wodurch sich Schadprogramme oft schnell und ungehindert weiterverbreiten können. Für den Netzbetreiber stellt sich deshalb zunehmend das Problem befallener Systeme. Im MWN beispielsweise bedeutet ein Anteil von einem Prozent an infizierten Rechnern rund 500 potientielle Verursacher von Störungen.

Neben den infizierten System im eigenen Netzwerk, finden zunehmend auch Angriffe aus dem Internet statt. Hier verfügt das MWN mit ca. 10 öffentlichen Class-B Netzen über einen vergleichsweise großen Adressraum, damit auch über eine entsprechend große Angriffsfläche. Auch hier verursachen ausgiebige Netzwerk-Scans, Infektionsversuche und gelungene Einbrüche, ausgehend von externen Systemen, zum Teil erhebliche Beeinträchtigungen bei den Nutzern im MWN.

In der Vergangenheit stellte die manuelle Bearbeitung solcher Problemfälle und die Benachrichtigung der Eigentümer oder entsprechender Netzverantwortlicher einen erheblichen personellen Aufwand dar. Auch führten die bisher eingesetzten technischen Maßnahmen nicht zu einem zufriedenstellendem Erfolg. Konkret wurden in der Vergangenheit Routerfilter, private IP–Adressen und klassische IDS/IPS eingesetzt. Im Folgenden werden diese Ansätze kurz vorgestellt, um deren Defizite zu analysieren.

1.1 Einsatz von Routerfiltern

Bei der Konfiguration von Routerfiltern können gezielt einzelne Ports oder IP-Adressbereiche gesperrt werden. Diese Maßnahmen sind dann erfolgreich, wenn sich die jeweilige Bedrohung anhand der Parameter IP-Adresse und Port eindeutig bestimmen lässt. So konnte in der Vergangenheit eine gute Wirkung gegen diverse Schadprogramme erzielt werden. Durch die manuelle Aktualisierung statischer Filterregeln entsteht allerdings ein ständiger und wiederkehrender Administrationsaufwand. Oft werden einzelne Ports gleichzeitig von Schadprogrammen aber auch von regulären Diensten verwendet, weshalb eine Portsperrung auch die berechtigte Nutzung von der

Dienstnutzung ausschließt. Aktuelle Schadprogramme machen zunehmend Gebrauch von Standardprotokollen auf den dafür vorgesehenen offiziellen Ports, so dass eine Portsperrung nicht mehr in Frage kommt. Genauso wenig wirksam erweisen sich solche portbasierenden Sperren da die Auswahl eines geeigneten Ports mittlerweile bei fast allen P2P-Clients dynamisch erfolgt.

Auch eine Verwendung dynamischer Paketfilter (häufig auch als reflexive Filter bezeichnet) an Subnetzen und Routerinterfaces führt zu Problemen. Bei dieser Filterart wird ein Verbindungskontext hergestellt. Dazu wird die Richtung in der eine Kommunikationsbeziehung aufgebaut wird mit berücksichtigt, um dann alle zu dieser Kommunikationsbeziehung gehörenden Pakete mit dynamisch erzeugten Regeln freizugeben. Wenn nun Schadprogramme eine große Zahl entfernter Hosts kontaktieren, um nach verwundbaren Systemen zu suchen oder Spam-Mails zuzustellen, muß eine große Anzahl von Verbindungsdaten im Router gespeichert werden. Ähnlich verhalten sich die meisten P2P-Protokolle. Sie bauen meist in kurzer Zeit eine große Zahl von Verbindungen auf und halten diese über viele Stunden hinweg. Dies kann jedoch zu gravierenden Einbußen hinsichtlich der Bandbreite und der Stabilität der beteiligten Router führen.

1.2 Private IP-Adressen

Durch die Vergabe privater IP-Adressen (ohne Network Adress Translation) können Hosts ohne gerouteten Übergang zum Internet betrieben werden. Damit diese dennoch auf Internetdienste zugreifen können, müssen aber sogenannte Proxy-Gateways eingesetzt werden. Diese Gateways (wie z.B. HTTP, FTP oder Circuit Level Proxies wie SOCKS) müssen dann speziell für jede Anwendung bereitgestellt und gewartet werden. Bei Protokollen, die nicht über vorhandene Proxies geleitet werden können, scheitert ein Internetzugriff neuer Dienste bei der Verwendung privater IP-Adressen völlig. Hierzu zählen beispielsweise oft eine Reihe von Voice over IP (VoIP) oder Videokonferenz–Protokollen wie z.B. H.323 oder SIP. Darüber hinaus können Proxies auch missbraucht werden, um Protokolle und Ports unerwünschter Anwendungen mit Hilfe von “Tunneling-Verfahren” ins öffentliche Netz zu übertragen. Besonders ungünstig wirken sich beispielsweise P2P-Protokolle über SOCKS-Proxies aus, die aufwändige Verbindungstabellen halten müssen. Diese Protokolle initiieren in der Regel eine hohe Anzahl von Verbindungen, was die Performanz und Betriebsstabilität des SOCKS–Dienstes gefährden kann.

Eine Filterung auf Virensignaturen, ohne speziell für jede einzelne Anwendung angebundenen Virenscanner, wird in der Regel nicht vorgenommen. Deshalb schafft eine Verwendung privater IP-Adressen im Hinblick auf die Virenproblematik keine zusätzliche Sicherheit.

Wie deutlich wird, muss bei konsequenter Fortführung des Ansatzes, private IP-Adressen im großen Rahmen einzusetzen und diese über Proxies nach aussen zu leiten, eine Vielzahl unterschiedlicher Proxy-Systeme betrieben werden. Trotzdem bleiben bei diesem Vorgehen immer eine Reihe nicht proxy-fähiger Dienste und Anwendungsprogramme, die dann in einer solchen Umgebung nicht verwendet werden können. Eine Vielzahl an möglichen Schadprogrammen ist ausserdem in der Lage, IP- und port-basierte Sicherheitsvorkehrungen durch Gateways zu umgehen.

1.3 Intrusion Detection und Prevention-Systeme

Durch den Einsatz von klassischen IDS/IPS wird der Netzverkehr mit Hilfe von Protokollanalysatoren und Mustererkennungsalgorithmen auf verdächtige Signaturen hin untersucht. Wird eine Signatur durch ein IDS erkannt, wird eine Meldung erzeugt. Darüber hinaus gibt es Systeme, die nur wenige oder keine Signaturen zur Erkennung verwenden und stattdessen auf statistische Methoden zur Analyse des Netzwerkverkehrs zurückgreifen. Beim IPS kann die betreffende Netzverbindung unterbunden werden. In verschiedenen Tests am LRZ wurden verschiedene IDS/IPS-Systeme auf ihre Alltagstauglichkeit untersucht. Getestet wurde sowohl Open-Source-Pakete [5, 1] als auch kommerzielle Systeme mit vielversprechenden Erkennungsfunktionen.

Da alle diese Systeme den gesamten Netzverkehr verfolgen und überprüfen müssen, zeigen sich deutliche Grenzen bei hohen Bandbreiten, Paketraten und Neuverbindungsraten. Zum Teil kommt es dabei zu hohen Paketverlusten, die besonders bei “Inline”-betriebenen Systemen problematisch sind. Hier werden lastbedingt beliebige Pakete beim Weg durch das System verworfen, was den Netzverkehr stark beeinträchtigt. Beim Einsatz solcher System müssen also vorher die maximalen Bandbreiten und Neuverbindungsraten auf dem betreffenden Netz bekannt

sein. Anhand dieser Vorgaben dürfen dann auf den IDS/IPS-Systemen gerade so viele Signaturen und Erkennungsverfahren ausgewählt werden, wie im schlechtesten Fall bei maximaler erwarteter Bandbreite noch ungehindert erkannt werden können.

Ein weiterer negativer Aspekt dieser Systeme betrifft die notwendige Auswahl der zu überwachenden Hosts, denn nicht alle Hosts im Netz zeigen das gleiche Kommunikationsverhalten. So werden an einem Fileserver sicher andere Signaturen und Protokolle geprüft werden müssen, als an einem Notebook-Computer mit Web-Browser. Deshalb müssen beim Einsatz von IDS/IPS-Systemen verschiedene Regelsätze für verschiedene Nutzungsprofile festgelegt und den betreffenden IP-Adressbereichen zugewiesen werden. Bei einem heterogenen und grossen Netz mit verteilter Verwaltung gestaltet sich dieses Vorhaben sehr schwierig oder gar unmöglich. Folglich können solche Systeme momentan nur für kleinere homogene Netzbereiche, wie z.B. von Arbeitsplatzrechnern, VPN-Zugangsnetzen oder auch Studentenwohnheimen effizient eingesetzt werden.

1.4 Folgerungen

Bei stetig steigendem Netzverkehr und zunehmenden Missbrauch von Infrastruktur und Endgeräten durch Würmer, Viren und P2P-Protokolle ist es absolut notwendig, Verfahren zur Behandlung dieser Probleme zu automatisieren. Ein weiterer Ausbau bestehender Sicherheitssysteme (z.B in Routern oder durch Proxy-Systemen) stellt keine befriedigende Lösung dar, weil so weder die Ursachen beseitigt, noch der Administrationsaufwand reduziert werden kann. Genausowenig ist eine weitere Einschränkung durch Portsperrungen zielführend, da die normale Netznutzung davon ebenfalls betroffen ist.

Im Gegensatz zu den bisher insgesamt reaktiven Problemlösungen wird also ein dynamisches, proaktives und generisches IPS mit einer Komponente zur dynamischen Bandbreitenbeschränkung gefordert. Ein solches System befindet sich seit Mitte 2005 erfolgreich im produktiven Einsatz am LRZ.

Im folgenden Abschnitt werden die Ziele des Konzepts, sowie die notwendigen Vorarbeiten dargestellt. Darauf folgend wird die Architektur unseres Systems vorgestellt. Abschnitt 5 beschreibt die technische Umsetzung. In Abschnitt 6 werden Ergebnisse und Erfahrungen des Produktivbetriebs vorgestellt. Abschnitt 7 gibt einen Ausblick auf weitere Fragestellungen in diesem Umfeld.

2 Ziele

Aus Erkenntnissen der bisherigen Ansätze und deren Schwächen lassen sich nun die folgenden Ziele für eine Lösung der genannten Probleme bestimmen:

- **Vereinfachung der bestehenden Strukturen:** Der Betrieb vieler differenzierte Hard- und Softwarekomponten und der damit verbundene personeller Aufwand muss verringert werden. Hier sollen wenige universelle Plattformen eingesetzt werden, deren Betrieb weitgehend automatisch möglich ist.
- **Verbreiterung des Dienstangebots:** Gleichzeitig sollen die Einschränkungen bei der Nutzung neuer Dienste (wie z.B. VoIP) aufgehoben werden und so eine größere Akzeptanz des neuen Konzepts erreicht werden.
- **Kontrolle der Netznutzung:** Die Automatisierung vieler Abläufe beim Betrieb eines Netzwerks muss vor allem Aspekte der Sicherheit berücksichtigen. Darüber hinaus müssen Bandbreiten und Volumina beim Netzwerkverkehr bis auf Basis einzeler IP-Adressen überwacht und ggf. beschränkt werden. Die manuellen Verfahren sollen durch neue Abläufe ersetzt werden, die sowohl die technischen Massnahmen (wie z.B. die Sperrung von IP-Adressen) als auch die notwendige Benachrichtigung der betroffenen Nutzer automatisieren. Die notwendigen Policies sollen auf einfache Weise festgelegt werden können. Verschiedene Analysemöglichkeiten sollen Aufschluss über Netzwerkverkehr, auffällige Systeme und aktive Policies geben.
- **Einfacher und sicherer Netzzugang:** Aus Sicht der Nutzer soll der Zugang zum Netzwerk möglichst unkompliziert sein. Die Einstellung von Proxyservern oder die Verwendung von speziellen Client-Programmen soll entfallen. Gleichzeitig erhalten die Benutzer einen Schutz vor Angriffen und eine Information, sobald ihr eigenes System ein auffälliges Kommunikationsverhalten zeigt. Hier soll ein möglichst

transparentes Verfahren eingesetzt werden, das den Benutzer in Echtzeit über Verstöße gegen die aktiven Policies informiert.

Grundlegendes Ziel ist der Betrieb des Netzes mit möglichst geringem manuellem Administrationsaufwand bei gleichzeitigem Ausbau der Nutzungsmöglichkeiten. Darüber hinaus soll der Netzzugang für den Benutzer deutlich vereinfacht werden bei gleichzeitiger Absicherung gegen Angriffe und Missbrauch.

3 Vorarbeiten

Um die oben genannten Ziele zu erreichen, ist es notwendig griffige Verfahren zu haben anhand derer eine Klassifikation des Netzwerkverkehrs möglich ist. Das Verhalten eines einzelnen Hosts im Netzwerk wird dazu anhand der folgenden Parameter klassifiziert.

Rate der (erfolglosen) Verbindungsaufbauversuche: Werden von einem Host in kurzer Zeit viele Verbindungen aufgebaut, so ist dies ein Zeichen für ungewöhnliche Aktivitäten. Besonders wenn diese Versuche vom jeweiligen Kommunikationspartner unbeantwortet bleiben, könnte es sich um einen Versuch handeln, andere verwundbare Systeme zu finden oder zumindest massiv zu beeinträchtigen.

Anzahl (aktiver) Kommunikationspartner: Unterhält ein Host viele Verbindungen zu unterschiedlichen Zielen, so könnte es sich auch hier um ein missbrauchtes System handeln. Mögliche Szenarien sind beispielsweise das Versenden von Spam-Mails oder auch die exzessive Verwendung von P2P-Verfahren. Dieses Kriterium gilt offensichtlich nicht für alle Systeme, wie z.B. Web-Server.

Sprunghaft ansteigende **Paketraten und Bandbreiten** sind meist auch ein Indiz für komprommitierte Systeme. Oft wird mit der maximal zur Verfügung stehenden Bandbreite ein Angriff auf andere Systeme vorgenommen. Genauso könnte z.B. ein Web-Server zum Ausliefern von Root-Kits oder für Phishing-Seiten missbraucht werden und damit unerwartet viel Verkehr produzieren.

Typische Ports stellten in der Vergangenheit ein griffiges Indiz für verwendete Dienste und deren Missbrauch dar. So konnten unerwünschte Aktivitäten durch einfache Portsperren unterbunden werden. Auch heute liefert die Verwendung bestimmter Ports einen Hinweis auf eine mögliche Komprommitierung von verwundbaren Systemen.

Protokollanalyse und typische Signaturen in den Nutzdaten geben letztlich Aufschluss über die Details einer Kommunikationsverbindung, die mit Hilfe rein statistischer Methoden nicht erfassbar wären.

Die oben aufgezeigten Kriterien verwenden vorwiegend statistische Methoden und nur wenige tiefergehende Analysen. Diese Verteilung im Ansatz wurde, aufgrund der Erfahrungen mit den bisherigen IDS-Systemen, absichtlich so gewählt: Signaturbasierte Verfahren erweisen sich als sehr resourcenhungrig, wodurch entweder nur wenige Signaturen oder nur geringe Paketraten bzw. Bandbreiten untersucht werden können.

Anhand dieser Vorgaben wurde im Rahmen der Vorarbeiten eine empirische Überprüfung von Netzwerkverkehr vorgenommen, um auffällige Systeme zu klasifizieren. Es wurde die Fragestellung untersucht, welche Kombination der oben genannten Kriterien griffige Anhaltspunkte zur Klassifikation und letztlich Grenzwerte zur Bestimmung von missbrauchten Systemen liefern kann.

Die empirische Analyse führte zu den folgenden Erkenntnissen:

- Alle untersuchten Parameter geben Aufschluss über potientiell kompromittierte Systeme. Optimal wäre eine vollständige Protokoll- und Nutzdatenanalyse in Echtzeit. Dies erweist sich jedoch in Netzen mit Bandbreiten $>$2Gbit/s als technisch schwierig realisierbar.
- Viele Systeme (z.B. Notebook-Computer) werden ausserhalb und innerhalb des MWN betrieben. Dadurch kann eine Komprommitierung eines Systems im Internet (z.B. an einem DSL-Anschluss) selbst bei bestem Schutz innerhalb des MWN nicht verhindert werden.
- Eine bestimmte Anzahl von missbrauchten Hosts verbleibt selbst bei Anwendung aller technischen Möglichkeiten in einem Netz dieser Größe. Ziel muss es sein, die Zahl möglichst gering zu halten.

Durch die gegebenen technischen Grenzen muss die Analyse des Netzwerkverkehrs auf Verfahren mit geringem

Resourcenbedarf (z.B. Hauptspeicher und Rechenleistung) eingeschränkt werden. Nur so kann das geforderte System auch bei hohen Bandbreiten und Paketraten noch zuverlässig funktionieren.

Auch lassen diese Ergebnisse den Schluss zu, dass totale Sicherheit und Kontrolle in einem Netz dieser Größe unmöglich sind. Ziel muss es sein das "Grundrauschen" durch infizierte Systeme möglichst gering zu halten. Konkrete Grenzwerte für kompromittierte Systeme müssen individuell für jede Policy bestimmt werden. Beispielsweise müssen bei HTTP-Anfragen höhere Neuverbindungsraten als bei bei SMTP-Transfers zugelassen werden.

4 Ein NAT-Gateway als IDS/IPS

Im Folgenden wird das System Nat-O-Mat vorgestellt, das als generisches IPS am Internet–Übergang des MWN zum Einsatz kommt. Ein solches IPS zeichnet sich in erster Linie dadurch aus, dass vorwiegend statistische Verfahren und nur wenige signaturbasierte Verfahren zum Einsatz kommen. Ein großer Teil infizierter Endsystemen lässt sich bereits mittels statistischer Verfahren erkennen, wodurch auf die weit aufwendigere Prüfung von Signaturen verzichtet werden kann. Dabei bestimmt das System verschiedene Parameter des Kommunikationsverhaltens auf Basis einzelner Hosts, ohne die verwendeten Protokolle oder übertragenen Dateninhalte im Detail kennen zu müssen. So wird erreicht, dass das IPS auch bei hohen Bandbreiten und Paketraten noch ohne Beeinträchtigungen arbeiten kann.

Einen besonderen Aspekt des vorgestellten Systems stellt die sog. "Sanfte Sperrung" dar. Hier handelt es sich um ein spezielles Verfahren, bei dem unerwünschter Verkehr nicht vollständig unterbunden, sondern in Abhängigkeit seiner Stärke nach einem Eskalationsprinzip gedrosselt wird. Dieses Verfahren wurde eingeführt, um kurzzeitigen Verstöße oder auch "False-Positive"-Fällen zu begegnen, ohne den Nutzer massiv einzuschränken oder gleich zu sperren. Somit verhält sich das System gerade bei nicht eindeutig festgestellten Verstößen kooperativ.

Darüber hinaus besitzt der Nat-O-Mat ein eigenes Reporting-System, bei dem sowohl Betreiber als auch Benutzer der Netzinfrastruktur beim Auftreten von Problemen direkt informiert werden können. Die direkte Information der Nutzer über erkannte Probleme soll bei der schnellen Behebung der Ursachen helfen und ein Bewusstsein für Gefahren durch Würmer und Viren aus dem Internet schaffen. Die Information des Betreibers dient zur Sicherstellung der Funktionsfähigkeit der Infrastruktur, falls ein Benutzer auf den Hinweis nicht in angemessener Weise reagiert.

Das System ist skalierbar ausgelegt, so dass eine Erweiterung bei steigender Auslastung ohne weiteres möglich ist. Bedingt durch die Tatsache, dass der Netzwerkverkehr über das System geleitet wird und ein Ausfall deshalb fatale Folgen hätte, besteht die Anforderung nach einer hohen Verfügbarkeit. Hierfür besitzt der Nat-O-Mat ein Redundanzkonzept mit Lastverteilung.

Im Folgenden werden die verschiedenen Grundfunktionen des Systems zuerst einzeln und dann im Zusammenhang beschrieben.

4.1 Grundfunktionen

Die Funktionsweise des IDS/IPS im Nat-O-Mat lässt sich grundlegend in zwei Teilbereiche gliedern: Policybasierte Analyse und Policy-Enforcement. Hinzu kommt eine Komponente zur dynamischen Bandbreitenregulierung im Rahmen des Policy-Enforcement.

Zuerst wird der Netzwerkverkehr anhand von festgelegten Regelsätzen (Policies) auf Host-Basis analysiert und klassifiziert. Die Klassifikation erfolgt nach einem Verfahren, das eine feine Abstufung der Auffälligkeit eines Systems zulässt. Die im ersten Schritt gewonnene Information über auffällige Hosts wird in einem zweiten Schritt (sog. Policy-Enforcement) in Reaktionen des IDS übersetzt. So können z.B. gezielt einzelne Hosts an der Kommunikation gehindert werden.

Alle nachfolgend beschriebenen Verfahren werden in Echtzeit auf den zu untersuchenden Netzwerkverkehr angewandt. Sie erlauben feingranulare Reaktionen basierend auf IP-Adressen einzelner Hosts bis hin zu einzelnen auffälligen Verbindungen oder Paketen.

4.2 Echtzeitanalyse des Verkehrs im Rahmen festgelegter Policies

Zu den wichtigsten Funktionen eines IDS/IPS gehört die Echtzeitanalyse des Netzwerkverkehrs. Hierzu müssen, je nach Policy, alle interessanten Pakete untersucht werden. Generell erfolgt die Festlegung der Policies beim Nat-O-Mat in Abhängigkeit von Subnetzbereichen und Ziel-Ports. Damit lassen sich beliebig viele Policies mit sehr feiner Granularität definieren. Je nach angewendetem Verfahren werden statistische Auswertungen oder auch Protokollanalysen und Signaturprüfungen vorgenommen. Der Nat-O-Mat verbindet sowohl statistische als auch tiefergehende Analyseverfahren, die im Folgenden genauer beschrieben werden.

Grundsätzlich werden drei Arten von Policies unterschieden:

- **Anzahl der Kommunikationsverhältnisse**
- **Paketraten und Bandbreiten**
- **Signaturen**

4.2.1 Statistische Verfahren

Bei den vom Nat-O-Mat eingesetzen statistischen Verfahren werden generell Paketraten bezogen auf einzelne Quell- oder Zieladressen und Ports betrachtet. Das System nimmt eine Echtzeitanalyse des Netzverkehrs auf Basis einzelner Hosts und Verbindungen vor. Das Verhalten eines Hosts im Netz wird dabei nach den folgenden Kritierien klassifiziert:

1. **Pakete, die zu keiner bekannten TCP-Verbindung oder keinem UDP-Flow gehören.** Hierzu gehören Scans von IP-Netzen, (D)DOS-Angriffe oder das Versenden von Spam-Mails. Generell werden zwei unterschiedliche Szenarien analysiert:
   - Rate der Pakete, die von einer Quelladresse an viele Zieladressen mit gleichem Zielport geschickt werden (DOS, Scan, Spam).
   - Rate der Pakete, die von vielen Quelladressen an eine Zieladresse geschickt werden (DDOS).
2. **Pakete aus bestehenden TCP-Verbindungen oder UDP-Flows** werden auf Paketrate bzw. Bandbreite hin untersucht.

Allein durch die Betrachtung von Paketraten lassen sich bereits viele infizierte oder zumindest auffällige Systeme ausmachen. Wichtig ist hier, dass alle Analysen auf Host-Basis stattfinden müssen. Für alle Regeln dürfen also nur Pakete von oder zu einem bestimmten Host betrachtet werden. Solche Analysen lassen sich durch Verwendung von Hash-Tabellen mit vertretbarem Aufwand betreiben. Typische Szenarien, die durch dieses Verfahren erkannt werden, sind beispielsweise andauernde Scans nach weiteren anfälligen Systemen oder das Versenden von Spam-Mails ausgehend von einem Host. Genauso erkannt werden komprommitierte Systeme, die z.B. über Bot-Netze ferngesteuert für DDOS-Attacken verwendet werden, um ein bestimmtes Ziel im Netz zu überlasten. Die empirischen Untersuchungen zeigen, dass die dabei auftretenden Paketraten in der Regel deutlich um mehr als den Faktor 10 über denen eines normalen Systems liegen.

Die Paketratenanalyse innerhalb bestehender Verbindungen lässt jedoch nicht einen direkten Rückschluss auf komprommitierte Systeme zu, da hierzu Kenntnisse über die Funktion des jeweilig analysierten Hosts im Netz vorhanden sein müssten. Beispielsweise empfängt ein Arbeitsplatz- oder Notebook-Computer in der Regel mehr Pakete, als er versendet. Bei einem Webserver wird dieses Verhältnis umgekehrt sein. Entspricht das Kommunikationsverhalten nicht diesen Erwartungen, so weist dies meist auf eine missbräuchliche Nutzung hin. Deshalb erfolgt auch hier eine Klassifikation der betroffenen Pakete bzw. Verbindungen für eine mögliche Reaktion im Policy-Enforcement. Verbindungen mit erhöhter Paketrate werden zudem von einer weitergehenden Analyse ausgenommen, um das IDS vor eventuellen Angriffen zu schützen. Auf diese Weise bleibt also auffälliger Verkehr im Zweifelsfall zu Gunsten der Konnektivität unbehandelt.

Die beschrieben Raten-basierten Policies können unterschiedlich je nach Protokoll und Port parametriert werden. So dürfen z.B. Verbindungen von einem Webbrowser (z.B. auf Port 80) mit höherer Rate neu aufgebaut werden, als die von einem Email-Client ausgehenden Verbindungen auf Port 25. Natürlich lassen sich diese Regeln auch mit den nachfolgend beschriebenen signaturbasiertenden Verfahren zu umfassenderen Policies kombinieren.

4.3 Signaturbasierte Verfahren

Etwas schwieriger gestaltet sich die Erkennung von P2P-Protokollen oder Bot-Netz-Protokollen. Hier erlaubt die statistische Betrachtung des Kommunikationsverhaltens allein keine zuverlässigen Aussagen. Deshalb muss hier eine vollständige Protokollanalyse vorgenommen werden. Gerade bei Systemen mit hohen Bandbreiten oder Paketraten benötigt eine vollständige Analyse viel Rechenzeit und Speicher. Um zu verhindern, dass ein DOS-Angriff gegen den Nat-O-Mat selbst erfolgt, werden verschiedene Begrenzungen bei der Analyse vorgenommen. So wird der Datenverkehr von/zu Hosts, die bereits bei der statistischen Auswertung auffällig geworden sind, nicht mehr durch signaturbasierte Verfahren analysiert. Grundprinzip des signaturbasierten Verfahrens ist es den zu untersuchenden Verkehr zu minimieren. Es wird nur der Datenverkehr einer Protokollanalyse unterzogen der nicht durch andere Heuristiken bereits als erlaubt oder verboten klassifizert werden konnte.

Die eigentliche Erkennung von Signaturen wird durch ein kernelbasiertes Screening-Verfahren unterstützt: Datenströme werden erst nach einem groben Test auf bekannte Muster an das eigentliche IDS weitergereicht. Auf diese Weise kann ebenfalls Rechenzeit und Hauptspeicher bei der Protokollanalyse eingespart werden. Darüber hinaus werden Datenströme innerhalb bestehender Verbindungen nur solange verfolgt, wie sie zur Erkennung einer entsprechenden Signatur notwendig sind.

Zur weiteren Verarbeitung werden die erkannten Signaturen einzeln klassifiziert, so dass eine differenzierte Auswertung und Weiterverarbeitung stattfinden kann. Dies ist notwendig, weil z.B. eine erkannte Bot-Netz Kommunikation sofort unterbunden werden muss, während P2P-Verbindungen lediglich in der Bandbreite beschränkt werden.

Generell kann auf diese Weise eine beliebige Anzahl von Policies, bestehend aus signaturbasierten und statistischen Verfahren individuell für beliebige Subnetze definiert werden. Es empfiehlt sich jedoch, die Policies anhand typischer Nutzungsszenarien (wie z.B. Server oder Arbeitsplatzrechner) zu definieren.

Während die statistischen Verfahren relativ einfach und sogar zustandslos funktionieren, hängt die Zuverlässig der signaturbasierten Verfahren jedoch von vielen Faktoren ab:

- Die **Qualität und Art einer Signatur** ist entscheident. Hier kann nicht für alle Protokolle die gleiche Zuverlässigkeit erreicht werden.
- Die **Vollständigkeit des Netzwerkverkehrs** ist nahezu bei allen Verfahren eine wichtige Voraussetzung, um auch eine vollständige Protokollanalyse betreiben zu können.
- Die **Anzahl und Art der aktiven Signaturen** in einem IDS entscheidet über die Nutzbarkeit und Auslastung des Systems.

Das Nat-O-Mat-System erlaubt die Kombination von statistischen und signaturbasierten Metoden zu beliebigen Regelsätzen (Policies). Einzelne Policies können wiederum zu einer neuen Policy kombiniert werden, um eine Verfeinerung oder Verstärkung des gesamten Regelsatzes zu bewirken. Policies selbst werden wirksam, indem sie auf bestimmte Subnetzbereiche oder Ports angewandt werden.

4.4 Maßnahmen bei Verstößen gegen Policies (Policy-Enforcement)

Der Nat-O-Mat sieht beim Verstoß gegen die vorher festgelegten Policies verschiedene Mechanismen nach einem Eskalationsprinzip vor. Damit eine individuelle Eskalation erfolgen kann, werden alle Verstöße gegen die aktiven Policies auf Host-Basis gezählt und in einem Strafpunktekonto festgehalten. Dieses Konto führt jedoch nur die Verstöße innerhalb eines gleitenden Zeitfensters (z.B. in den letzten 15 Minuten). Ältere Verstöße bleiben unberücksichtigt. Der Strafpunkt-Kontostand dient als Basis für alle Maßnahmen des Policy-Enforcement. So beziehen sich alle nachfolgend erläuterten Grenzen wie z.B. bei Sperrung, Freischaltung oder Benachrichtigung darauf. Grundsätzlich erfolgen alle Maßnahmen automatisch, ohne manuellen Eingriff, anhand eines 4-stufigen Verfahrens:

1. Werden die festgelegten Policies nur kurzzeitig überschritten, so wird dies als kein Verstoß gewertet. Mit der sog. **Burst-Bedingung** wird eine Toleranz gegenüber kurzfristigen Abweichungen im Kommunikationsverhalten erreicht.

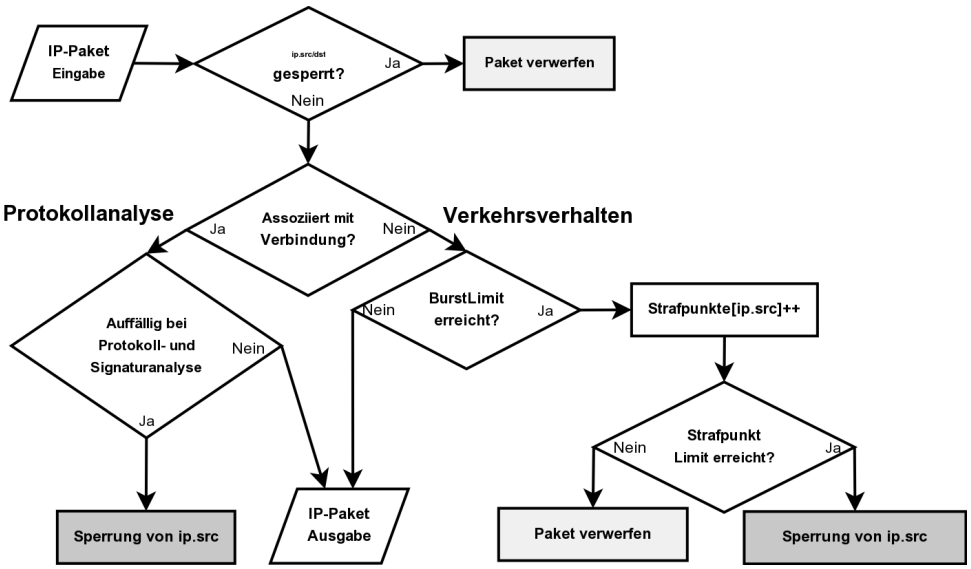

Abbildung 1: Schematisches Ablaufdiagramm

2. Hält die Überschreitung der Policies länger an, als in der Burst-Bedingung festgelegt, so wird ein sog. **Soft-Limit** erreicht, bei dem alle nachfolgenden Pakete verworfen werden. Diese Sperrung bleibt solange aufrechterhalten, wie die Ratenüberschreibung anhält. Mit Erreichen eines Soft-Limits wird für die verursachende IP-Adresse in regelmäßigen Abständen ein Strafpunkt erteilt und zwischengespeichert.

3. Die nächste Eskalationsstufe, das sog. **Hard-Limit**, wird erreicht, sobald eine bestimmte Zahl von Strafpunkten überschritten wird. Nun erfolgt eine Sperrung der verursachenden IP-Adresse durch das Nat-O-Mat-System. Anschliessend werden alle HTTP-Anfragen des Rechners mit der gesperrten IP-Adresse auf eine Informationsseite umgeleitet, die den betroffenen Benutzer über die Sperrung und die möglichen Ursachen informiert (Abbildung 2). Darüber hinaus wird dieser Vorgang vom System protokolliert, so dass auffällige Systeme schnell vom Administrator aufgefunden werden können. Die Sperrung wird erst dann wieder aufgehoben, wenn die Anzahl der Strafpunkte innerhalb eines gleitenden Zeitfensters unter das Hard-Limit fällt. Vorraussetzung dafür ist, dass der das Hard-Limit auslösende Datenstrom beendet wird. Dies kann der Benutzer beispielsweise durch Entfernen des Virus, abschalten oder umkonfigurieren der P2P-Software o.ä. erreichen.

4. Die vierte Eskalationsstufe, die sog. (**organisatorische Eskalation**), tritt in Kraft, wenn ein System nach Erreichen des Hard-Limits für längere Zeit weiter auffällig bleibt. In diesem Fall wurden vom Benutzer des Systems offensichtlich keine eigenen Gegenmaßnahmen eingeleitet. Deshalb wird mittels einer Datenbank ein verantwortlicher Ansprechpartner für den betroffen IP-Adressraum ausgemacht und per Email über den Verstoß gegen die Policy informiert. In der Regel wird über diesen Weg ein Netzverantwortlicher vor Ort mit der Beseitigung des Problems beauftragt.

Status Report for 129.187.47.34 (gesperrt/blocked)

Überschreitungen Number of hits	Protokoll Protocol	Zielport und Grund der Sperrung Destination port and suspension reason
105	ICMP	Zu viele Pings
63	TCP	25 SMTP, Versenden von zu vielen Spam- oder Virenmails
33	TCP	6600-6699 WinM / Napster Filesharing
21	TCP	53 DNS, Zu viele DNS Anfragen

Abbildung 2: Benutzerinformation

4.4.1 Anmerkungen

Befindet sich der Verursacher eines Verstoßes in einem externen Netz (z.B. dem Internet), werden zwar Sperrungen vorgenommen, jedoch steht dem Verursacher kein abrufbarer Report zur Verfügung. Es erfolgt auch keine automatische Benachrichtigung an einen Administrator. Bei Bedarf kann jedoch eine manuelle Bearbeitung erfolgen.

Die Toleranz des Systems gegenüber Verstößen ist abhängig von der Art des Verstoßes. Zum Beispiel führt eine erkannte Bot-Netz-Kommunikation direkt zur dritten Eskalationsstufe, also der Sperrung des jeweiligen Hosts.

Das Konzept der sanften Sperrung nach dem oben beschriebenen Eskalationsverfahren ist in Abbildung 1 dargestellt. Deutlich zu erkennen ist die klare Trennung zwischen statistischen und signaturbasierten Verfahren.

4.5 Bandbreitenregulierung und anwendungsorientierte Priorisierung

Das Policy-Enforcement im Nat-O-Mat-System wurde um eine Bandbreitenbeschränkung erweitert, die unabhängig von den beschriebenen Eskalationsstufen funktioniert. Sie erlaubt die Einordnung einzelner Verbindungen in verschiedene Bandbreitenklassen. Dies ist besonders dann interessant, wenn die maximal zur Verfügung stehende Netzwerkbandbreite anwendungsorientiert kontingentiert oder priorisiert werden soll. Auf diese Weise können z.B. den vorab durch Signaturanalyse klassifizierten P2P-Protokollen individuelle Bandbreiten oder Prioritäten zugewiesen werden.

Dabei kann die Bandbreite für alle Hosts (z.B. in einem Subnetz) oder allein auf Host-Basis begrenzt werden. Aus Gründen der einfacheren Verwaltung empfiehlt sich jedoch die erste Variante.

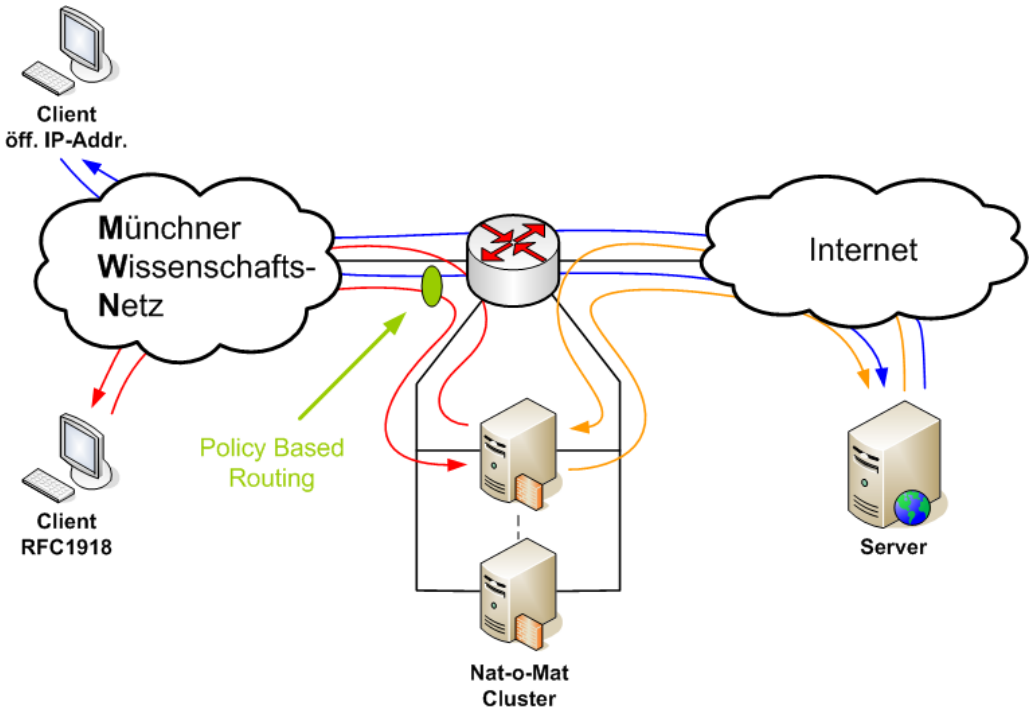

Abbildung 3: Policy-based Routing

5 Technische Realisierung

Das Nat-O-Mat-System wurde als Cluster von Linuxrechnern auf einer 64Bit x86-Plattform implementiert. Alle Einzelsysteme wurden über Heartbeat [6] hochverfügbar gemacht. Jedes System im Cluster ist identisch konfigu-

riert und arbeitet als Router, jedoch mit eigenen IP-Adressen. Wird mehr Netzbandbreite oder Rechenleistung für die Bewältigung der Aufgaben benötigt, so kann das Cluster durch weitere Einzelsysteme erweitert werden.

Um Netzverkehr über ein System in diesem Hochverfügbarkeits-Cluster zu leiten, werden die betreffenden Netze durch den Einsatz von Policy-Based Routing vom X-WiN-Zugangsrouter des Leibniz-Rechenzentrums auf eine virtuelle IP-Adresse im Cluster geroutet (siehe Abbildung 3). Fällt ein System aus, so bewirkt der Heartbeat-Mechanismus die Übernahme der IP-Adresse des betroffenen Systems auf ein anderes System im Cluster. Hierdurch werden, da derzeit noch keine stabilen Implementationen für das Mirroring der NAT-Informationen verfügbar sind, lediglich laufende TCP-Verbindungen von NAT-benutzenden Clients zurückgesetzt, während UDP-Datenströme und Verbindungen von gerouteten Netzen mit offiziellen IP-Adressen in den meisten Fällen nahezu unterbrechungsfrei weiterlaufen.

Die eigentliche IPS-Funktionalität mit den oben genannten Eigenschaften wird mit Hilfe von Netfilter/iptables [7] und Traffic-Control [3] erbracht. Zur Erkennung von Botnetz-Clients wird Bro [1] eingesetzt. Zur Verwaltung und Umsetzung der Policies wurden Shell und Perl-Skripte entwickelt. Darüber hinaus verfügt der Nat-O-Mat über ein umfangreiches Webinterface zur Analyse des laufenden Verkehrs und zur Anzeige von Verstößen gegen die Policies. Zusätzlich erfolgt eine grafische Darstellung von Statistiken durch RRD-Graphen [4] (siehe Abbildung 4.

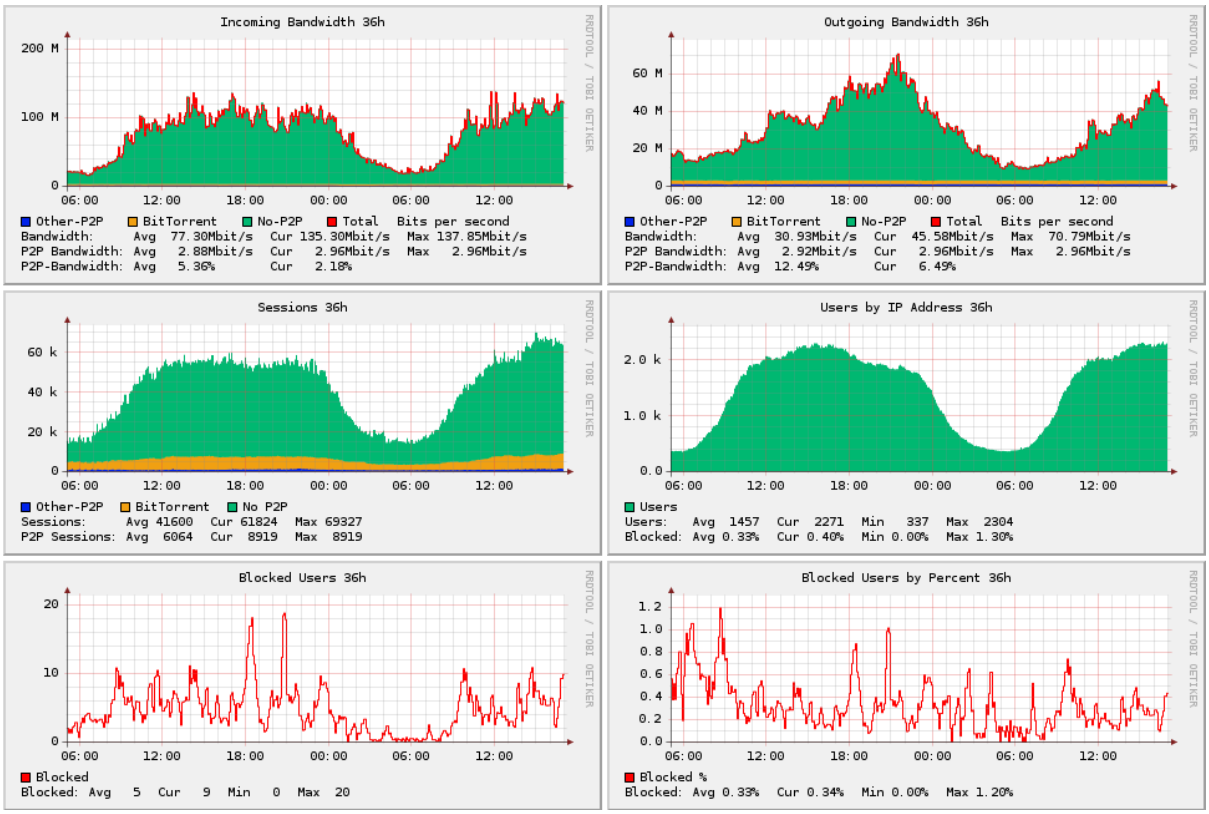

Abbildung 4: Verteilung von Bandbreiten und Auffälligkeiten im Tagesverlauf

6 Zusammenfassung und Ergebnisse

Das vorgestellte System bietet IPS-Funktionen, die auch bei hohen Bandbreiten und Paketraten noch zuverlässig arbeiten. Dies wird erreicht, indem verschiedene Analysetechniken so kombiniert werden, dass eine vollständige Protokollanalyse, sowie die Überprüfung von aufwendigen Signaturen weitgehend entfallen kann. Ein so konzipiertes IPS arbeitet im Vergleich zu herkömmlichen Systemen mit einer etwas geringeren Trefferquote, wodurch lediglich eine “Best-Effort”-Wirkung erzielt werden kann. Trotzdem werden mit hoher Zuverlässigkeit deutlich auffällige Hosts identifiziert und gesperrt. Ohne den Einsatz eines solchen Systems wären z.B. Portsperrungen

notwendig, von denen auch der reguläre Netzverkehr betroffen wäre. Der Nat-O-Mat nimmt zudem alle Sperrungen automatisch vor und informiert Benutzer und Administratoren automatisch. Somit entsteht kein Aufwand mehr bei der Bearbeitung von Störungen, die durch auffällige Rechner auftreten.

Der Nat-O-Mat befindet sich seit Juni 2005 am Leibniz-Rechenzentrum München im Produktionseinsatz zum Schutz von VPN-Zugangsnetzen, Computern in Poolräumen und Studentenwohnheimen. Pro Einzelsystem des Clusters werden täglich ca. 700 Gbyte Daten bei Datenraten von bis zu 200Mbit/s übertragen. Dabei werden bis zu 50.000 Verbindungen auf Verstöße gegen die eingerichteten Policies untersucht. Gleichzeitig aktiv sind bis zu ca. 2.500 Hosts, von denen im Mittel 0,5% auffällig und gesperrt sind. Pro Tag nimmt ein System ca. 3.500 temporäre Sperrungen und weniger als 10 Email-Benachrichtigungen an die Administratoren vor.

Beschwerden über zu unrecht gesperrte Rechner traten bisher fast keine auf. Nur bei Versuchen mit Applikationen wie Onlinespielen, die im Rahmen des LRZ Dienst-Portfolios nicht unterstützt werden, da eine wissenschaftliche Netznutzung im Vordergrund steht, kam es in wenigen Fällen zu “False Positives”. Insgesamt wurde das System seit seiner Einführung sehr positiv aufgenommen, nicht zuletzt deshalb, weil aus Nutzersicht der Konfigurationsaufwand für Gateways und Proxies wegfällt und, beispielsweise bei FTP-Verkehr, auch höhere Datentransferraten erreicht werden. Viele Benutzer erfahren ausserdem erst bei einer Sperrung auf der Informationsseite von einer möglichen Infektion ihres Rechners, was ebenfalls sehr gut aufgenommen wird.

7 Ausblick

Der Betrieb des Nat-O-Mat Systems an zentraler Stelle bietet sowohl Vor-, als auch Nachteile: In erster Linie steht dabei die einfachere Wartung und Konfiguration eines zentralen Systems im Vordergrund. So müssen z.B. Policies nur an einer Stelle konfiguriert und IP-Routen nur an einem Router angepasst werden. Trotzdem ergeben sich bei entsprechender Netzgröße auch Nachteile, da bei einem zentralem Aufbau lediglich Netzwerkverkehr von und zum Internet vom Nat-O-Mat analysiert werden kann. Damit existiert für die gesamte netzinterne Kommunikation keine IPS-Funktionalität.

Dieses Problem könnte durch den Einsatz von MPLS mit Layer3-VPNs umgangen werden, wodurch Gruppen von Subnetzen (beispielsweise Lehrstuhlnetze, Studentenwohnheime und Konferenznetze) zu virtuellen Netzen zusammengefasst werden. Der Nat-O-Mat könnte dann auch zur Absicherung dieser virtuellen Netze untereinander eingesetzt werden. Durch derartige Erweiterungen der Netzinfrastruktur wäre auch eine Verteilung von Nat-O-Mat Systemen an den Netzrand denkbar. Dieser dezentrale Ansatz erfordert jedoch eine Weiterentwicklung des bisherigen Systems. Hierfür müsste zuerst eine Trennung zwischen Policy-Management und Policy-Enforcement stattfinden. So kann erreicht werden, dass an zentraler Stelle eine Verwaltung der Policies stattfindet, während die Ausführung der IPS-Funktion dezentral erfolgen kann. Darüber hinaus könnte ein zentrales Logging aller erfassten Vorgänge im dezentralen System eine weitergehende Korrellation von sicherheitsrelevanten Informationen ermöglichen. Einige existierende IDS Systeme verwenden einen ähnlichen Ansatz, bei dem sog. Sensoren die Rolle der abgesetzten Erfassungssysteme übernehmen.

8 Danksagung

Die Autoren danken den Mitgliedern der Gruppen Netzbetrieb und Netzplanung des Leibniz-Rechenzentrums München, dem Lehrstuhl Prof. Feldmann (TU München) und dem Münchener Netzwerk-Management Team (MNM Team) unter Leitung von Prof. Hegering für hilfreiche Diskussionen und wertvolle Kommentare.

Literatur

[1] Bro Intrusion Detection System, `http://www.bro-ids.org/`.

[2] Leibniz Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ), `http://www.lrz.de`.

[3] Linux Advanced Routing & Traffic Control, `http://www.lartc.org/`.

[4] RRDtool - Logging & Graphing, http://www.rrdtool.org.

[5] snort.org — open source network intrusion prevention and detection system, http://www.snort.org/.

[6] The High-Availability Linux Project, http://www.linux-ha.org/.

[7] The netfilter.org project, http://www.netfilter.org/.

[8] V. Apostolescu and A. Läpple. Das Münchner Wissenschaftsnetz (MWN) — Konzepte, Dienste, Infrastrukturen, Management. Technical report, Leibniz-Rechenzentrum, December 2004, http://www.lrz-muenchen.de/services/netz/mwn-netzkonzept/mwn-netzkonzept.pdf.