Sicherheit im Backbone-Netz durch Firewalls & Co.

Steffen Schatz | steffen.schatz@cms.hu-berlin.de

Ausgehend von allgemeinen Sicherheitsbetrachtungen gibt dieser Artikel einen Einblick zum Einsatz von Firewalls, Routern und eines Traffic-Management-Systems im Netz der HU. Dabei werden auch kurz die verwendeten Geräte vorgestellt.

Allgemeines

An die Netzwerkinfrastruktur der Humboldt-Universität werden hohe Anforderungen gestellt, da sie eine unverzichtbare Arbeitsgrundlage für Lehre, Forschung und Verwaltung unserer Universität ist. Die IT-Infrastruktur soll einerseits eine größtmögliche Flexibilität und Offenheit im Rahmen von Forschung und Lehre bieten und auf der anderen Seite soll die Verfügbarkeit von Netzwerkressourcen, Daten und Diensten gewährleistet sein. Das ist ein gewisser Widerspruch, denn die Infrastruktur ist anfällig gegenüber vielen Bedrohungen. Risiken liegen insbesondere im Verlust der Verfügbarkeit, im Missbrauch der Systeme durch unautorisierte Benutzer bzw. durch externe Angreifer (z. B. für Angriffe auf Ziele innerhalb und außerhalb des HU-Netzes) und im Verlust der Vertraulichkeit bzw. der Integrität von Daten. Aus diesen Risiken können sich als Konsequenz für die HU der Verlust von Produktivität, Werten und Ansehen, aber auch eine Schädigung Dritter ergeben. Daraus resultieren die Anforderungen an die Sicherheit der IT-Infrastruktur.

Dieser Beitrag konzentriert sich auf die Darstellung unserer Maßnahmen zur Sicherung des Backbone-Netzes. Die Sicherheit der Netze der HU-Einrichtungen wird zum einen durch die Absicherung des Backbone-Netzes bestimmt, andererseits sind die Sicherheitsanforderungen der Teilnetze sehr verschieden. Ihre Absicherung kann, sofern erhöhte Anforderungen bestehen, nur in Zusammenarbeit zwischen den Einrichtungen und dem CMS erfolgen.

Die IT-Infrastruktur des Backbone-Netzes der HU wird durch Firewalls, Router und ein Traffic-Management-System geschützt.

Die HU hat zwei Verbindungen zum Internet: die aktive über den Campus Adlershof und eine Backup-Verbindung über den Campus Mitte. Am Übergang vom Internet zum HU-Netz in Adlershof arbeitet ein Traffic-Management-System (P2P-Filter). Das ist ein Gerät, welches zum Monitoring und Verwalten von Datenströmen bis hin zur Anwendungsebene benutzt wird. Dann folgt ein Firewall-Cluster, der gleichzeitig auch als Hauptrouter fungiert. Über einen zweiten Firewall-Cluster im Hauptgebäude in Mitte gibt es eine Backup-Verbindung ins Internet. Der Cluster in Adlershof wickelt metrikgesteuert den gesamten Datenverkehr zum Internet ab, während der andere für die Firewall-Aufgabe als Standby-Gerät bereitsteht und bei einem Ausfall den ersten Cluster ersetzt.

Die Backbonerouter sind über ein vermaschtes Netz (siehe Beitrag über das Backbone-Netz in diesem Journal) miteinander verbunden. Als letztes folgen dann in den Standorten die dortigen Router.

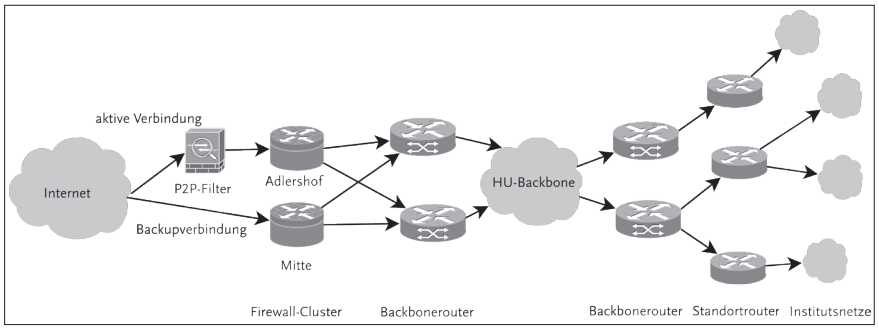

Abb. 1: Übersicht zum HU-Netz

Traffic-Management-System

Mit dem Traffic-Management-System ist eine effektive Erkennung, Bandbreitenverwaltung und Optimierung von Netzwerkanwendungen möglich. So können viele Protokolle für Peer-to-Peer-Tauschbörsen (P2P), Instant-Messaging-Dienste (IM), Voice over IP (VoIP), Tunneling und Mediastreaming, aber auch für herkömmliche Internetanwendungen verwaltet werden. Bei uns arbeitet das System vor allem als P2P-Filter, so dass wir auch diesen Namen verwenden. Die folgenden Hinweise zu den Protokollen und Diensten, die mit dem Traffic Management beeinflussbar sind, sollen den Einsatzzweck des Systems erläutern.

P2P

Peer-to-Peer-Dienste verbrauchen heute eine erhebliche Bandbreite im Internet. Das verursacht nicht nur steigende Kommunikationskosten, sondern beeinträchtigt auch die Qualität und Verfügbarkeit von anderen Anwendungen im Netz, wie zum Beispiel Internettelefonie, Web-Dienste oder E-Mail. Dabei ist auch zu beachten, dass durch P2P-Dienste viele urheberrechtlich geschützte Daten getauscht werden. Mittels einer gezielten Prioritäts- und Datenratensteuerung lässt sich der Anteil von P2P-Traffic eingrenzen. Zu den erkannten Diensten zählen bekannte wie Kazaa, eDonkey, BitTorrent und Gnutella, aber auch exotische und neue wie OFF und XDCC.

IM

Instant-Messaging-Dienste werden im Internet stark genutzt. Aber dieser Gebrauch erzeugt auch ernste Sicherheitsrisiken, da sie auch zur Verbreitung von Würmern und Viren, für DDoS-Attacken und als Plattform für Botnetze verwendet werden. Beispiele für bekannte IMS sind IRC, MSN, OSCAR, Yahoo und Jabber/Google Talk.

VoIP/Skype

Voice over IP (VoIP), dabei insbesondere Skype, ist eine der beliebtesten Anwendungen im Internet. VoIP-Anwendungen werden am stärksten durch überlastete Netze beeinträchtigt. Ihre Qualität kann durch die Vergabe von Prioritäten und garantierten Bandbreiten mittels des Traffic-Managers sichergestellt werden. Beispiele für bekannte VoIP-Dienste sind Fring, H.323, Skinny, Skype, RTCP, SIP.

Streaming

Ein Teil des Netzverkehrs wird durch Media-Streaming-Protokolle erzeugt, wie sie von Internetradio, TV-Stationen und vielen Webseiten benutzt werden. Diese Dienste sind inzwischen sehr beliebt und werden zunehmend genutzt. Beispiele dafür sind FLASH, MPEG, PPLive, PPStream, QuickTime, RTP, RTSP, Windows Media Stream, Zattoo.

Tunnel-Protokolle

Tunnelprotokolle, wie OpenVPN oder IPSec, werden dazu benutzt, Daten über das Internet sicher zu übertragen. Während es praktisch unmöglich ist, verschlüsselte Tunnel zu dechiffrieren und den Verkehr innerhalb des Tunnels zu analysieren, kann das Tunnelprotokoll selbst ermittelt und kontrolliert werden. So kann zum Beispiel der Verkehr eines Tunnelprotokolls auf bestimmte Endpunkte eingeschränkt werden, um einerseits die sichere Übertragung zu ermöglichen, andererseits den Missbrauch von Tunneln zu verhindern.
Beispiele für Tunnelprotokolle sind GRE, HamachiVPN, IPSec, L2TP, OpenVPN, SSL, Tor, SSH.

Spiele-Protokolle

Viele populäre Spiele benutzen Gaming-Protokolle. Der Traffic-Manager kann dazu benutzt werden, Online-Spiele z. B. an Schulen oder Universitäten zu blocken.

Beispiele für solche Online-Spiele sind Battlefield, Halo, Quake, Second Life, World of Warcraft, XBox.

Standard-Internetanwendungen

Hiermit sind die wichtigsten Protokolle für Web, E-Mail, Dateitransfer, Fernzugriff und netzinterne Protokolle wie Routing, Netzwerkfilesysteme und NTP gemeint.

Traffic-Management an der Humboldt-Universität

Mit Hilfe von einfachen Filterregeln können somit einzelne Dienste/Dienstgruppen gebremst oder geblockt werden. Damit kann die Verfügbarkeit des allgemeinen Netzes sichergestellt werden.

Unser Traffic-Management-System ist ein PRX-5G der Firma ipoque. Das Gerät interpretiert Netzwerkverkehr sehr zuverlässig mit einer Kombination aus Deep Packet Inspection (DPI) und Verhaltensanalyse – unabhängig davon, ob die Protokolle und Anwendungen verschlüsselt sind oder nicht. Die Filter arbeiten protokollbasiert und erkennen z. B. P2P-Verkehr an seinem charakteristischen Fingerabdruck in den Datenpaketen. Frühere Lösungen basierten meist auf Firewall-Systemen, die den Datenverkehr hinsichtlich bestimmter TCP- und UDP-Portnummern herausfiltern. Die ipoque-Technik ist im Vergleich dazu weniger fehleranfällig, und Fehlklassifikationen werden durch die Paketanalyse relativ gut vermieden. Bei uns ist das Gerät mit 1 Gbit/s angeschlossen. Ein optischer Hardware-Bypass sorgt dafür, dass der PRX-5G bei einem Defekt überbrückt wird. Bei Verwendung von 10-Gigabit-Schnittstellen kann das Gerät Datenverkehr bis zu 4 Gbit/s bearbeiten, ohne dass es zu einer merklichen Latenz der Datenpakete kommt. Da wir im Moment einen Internet-Zugang mit einer Bandbreite von 900 Mbit/s besitzen und die aktuellen durchschnittlichen Datenraten bei 300–400 Mbit/s liegen, ist also mit einer Leistungseinbuße nicht zu rechnen.

Firewall-Cluster

Ein Firewall-System schützt ein inneres Netz gegen Angriffe von außen, z. B. unser Universitätsnetz gegen das Internet. Es steht an der Übergangsstelle zwischen äußeren und inneren Netzen. Mit der Einrichtung eines Firewall-Systems soll eine gewisse Sicherheitsstufe für das interne Netz erreicht werden, so dass sich der Endgeräteschutz wirkungsvoll erhöht. Firewalls unterstützen ferner das Erkennen von Angriffen

durch umfangreiches Logging und Screening (Beobachtung der Datenströme). Firewall-Systeme lassen sich in drei Haupttypen unterscheiden: einfache Packet-Filter, Stateful Inspection Gateways und Application Level Gateways.

Ein Packet-Filter arbeitet in der Regel auf der Netzwerk- und der Transportschicht (IP bzw. TCP/UDP). Als aktives Netzwerkgerät leitet er Datenpakete in ein Netzwerk hinein bzw. aus einem Netzwerk hinaus und filtert diese zusätzlich nach erlaubten und unerlaubten Quell- und Zieladressen (IP-, ICMP-Header) sowie nach Quell- und Zielports (TCP-, UDP-Header).

Eine Stateful Inspection Firewall (SI-Firewall) analysiert die Pakete der Transportschicht und speichert in internen Tabellen zustandsabhängige Daten über neu aufgebaute Verbindungen (Sessions). Der Abgleich eingehender Pakete mit der Zustandtabelle erlaubt es, Pakete zu blocken, die weder eine neue Session aufbauen noch zu einer vorhandenen gehören.

Ein Application Level Gateway arbeitet auf der Anwendungsschicht. Es befindet sich quasi transparent zwischen Server und Client und stellt für den Server den Client dar und umgekehrt. Das bedeutet, dass die Verbindungspartner über dieses Gateway miteinander kommunizieren (Proxy-Prinzip). Der Nutzer hat jedoch den Eindruck, er kommuniziere direkt mit dem Zielrechner. Für jeden TCP/UDP-Dienst wird ein eigener Proxy benötigt. Proxys haben den Vorteil, dass sie sicherheitstechnische Prüfungen auf Applikationsebene durchführen und bei einer Fehlfunktion keine Sicherheitslücke darstellen (es wird dann lediglich die Kommunikation der Applikation unterbunden).

Firewalls sind in der Regel mehrstufig aufgebaut. Zum Beispiel werden zwei Packet-Filter mit einem Application Level Gateway kombiniert. Dieses Konzept nennt man auch Screened Gateway. Zusammengefasst in einem Gerät wird es z. B. von Juniper als „Integrated Security Gateway“ bezeichnet. Die Geräte dieser Firewall-Klasse bieten neben den genannten Firewall-Funktionen meistens erweiterte Routing-Funktionen und weitere Sicherheitsfunktionen (Intrusion Detection and Prevention, VPN-Gateway, tiefgehende Screening-Funktionen, VLANs und virtuelle Router).

Wir verwenden als Firewalls die Systeme ISG 2000 und ISG 1000 der Firma Juniper. Beides sind SI-Firewalls, die zusätzlich umfangreiche Sicherheitsfunktionen wie Deep Inspection, dynamisches routenbasiertes VPN, Network Address Translation (NAT), Virtualisierungs-Funktionen, erweiterte Routing-Protokolle (BGP, OSPF) sowie ein vollständiges IDP-System (Intrusion Detection and Prevention) bieten. Darüber hinaus beschleunigen spezielle Prozessoren Features wie Schutz vor Denial-of-Service-Attacken und andere Screening-Funktionen. Weitere Funktionen lassen sich per Software-Optionen integrieren. Zurzeit werden die ISG-Systeme nur als Firewall und Eingangsrouter zum HU-Netz benutzt.

Wir haben im Backbone-Netz der HU zwei Firewall-Standorte, einen in Adlershof (Zugang zum Internet über das Deutsche Forschungsnetz X-WiN) und den anderen im Hauptgebäude in Mitte (Zugang zum Internet über das Berliner Wissenschaftsnetz BRAIN). Damit ist bei Ausfall eines Standortes die Internetverbindung über den anderen gewährleistet. In diesen Standorten ist jeweils ein Firewall-Cluster aufgebaut, in Adlershof ein Firewall-Cluster aus zwei ISG 2000 und in Mitte ein Cluster aus zwei ISG 1000. Die ISG 1000 erzielt bei reinem Firewall-Betrieb 2 Gbit/s Datendurchsatz für alle Paketgrößen und die ISG 2000 schafft 4 Gbit/s. Das ist für die Bandbreite unseres Internetzugangs und die aktuelle Auslastung ausreichend. Zurzeit sind auf den Clustern 300 Policys und 600 registrierte IP-Adressen eingetragen.

Die Geräte sind paarweise als aktiv/passiv-Cluster aufgebaut, das heißt, ein Gerät befindet sich im Hot-Standby, das andere arbeitet und synchronisiert ständig die aktiven Sessions mit dem passiven Gerät. Dadurch ist bei Ausfall des aktiven Gerätes innerhalb des Clusters eine komplette Session-Übernahme ohne Unterbrechung für den Nutzer gegeben.

An die Firewalls sind Router des Backbone-Netzes sowie spezielle Teilnetze der HU angeschlossen. Letztere sind z. B. Management-Netze, technische Netze für Zutrittskontrolle und Gebäudeleittechnik usw. Sie sind gesondert abgesichert und nur von bestimmten Nutzern, Diensten und Rechnern benutzbar.

Der Zugriff von außerhalb auf Rechner und Ressourcen des HU-Netzes wird bis auf die allgemeinen Standarddienste wie z. B. SSH, HTTP, HTTPS oder FTP geblockt. Da dies für einige Nutzer nicht reicht, gibt es auch Ausnahmen, die in Absprache mit dem CMS vereinbart wurden. Zu den Diensten, die generell von außen nicht erreichbar sind, zählen z. B. die Ports 135–139, die durch verschiedene Windows-Dienste benutzt werden. Auch NFS, RPC und SMB sind zum Internet gesperrt. Damit sind viele Übertragungswege für Schadsoftware, Würmer, Trojaner usw. geschlossen.

Innerhalb der HU betreiben wir ein relativ offenes Netz. Die meisten Standarddienste sind ohne Reglementierungen nutzbar und werden von den Firewall-Clustern nach draußen durchgelassen. Es gibt auch Ausnahmen, wie zum Beispiel SMTP (Mailversand). Dafür sind nur die offiziellen Mailserver der HU zugelassen. Damit ist ein beabsichtigter oder unbeabsichtigter SPAM-Versand aus unserem Netz heraus erschwert. Die Regeln sind bis auf einige Ausnahmen auf beiden Firewall-Clustern gleich.

Die ISGs verfügen über viele Screening-Funktionen, die den Datenverkehr auf Anomalien beobachten. Damit können die Firewalls sich selbst, aber auch das HU-Netz vor vielerlei Attacken (Packet-Flooding, Teardrop, Ping of Death, Land Attack, WinNuke, manipulierte ICMP- und IP-Pakete usw.) schützen, indem diese geblockt werden. Solche Attacken können einzelne Rechner wie auch ganze Netze lahmlegen. Diese Screening-Funktionen beanspruchen aber viel Leistung, so dass nach einer Testphase einige wieder deaktiviert wurden.

Auf den ISG-Systemen wird NAT eingesetzt, um eine Kommunikation von Clients mit privaten IP-Adressen nach außen zu gestatten. Dies ist beispielsweise für Angehörige fremder Einrichtungen wichtig, wenn sie den CASG-Verbund des DFN-Vereins aus dem HU-WLAN nutzen wollen.

Ein Sonderfall ist das Verwaltungsnetz der HU. Dieses ist durch ein gesondertes Firewall-System vom übrigen HU-Netz abgeschottet.

Backbonerouter

Im Backbone-Netz verwenden wir Geräte aus der MLX-Familie von Foundry. Die Hauptaufgabe der Router ist die Datenkommunikation innerhalb des HU-Netzes. Auf ihnen sind keine Access-Listen installiert, die den Datenverkehr der angeschlossenen Institute reglementieren. Lediglich die Restriktionen für das WLAN HU-VPN (Kommunikation nur zu VPN-Gateways) werden auf ihnen umgesetzt. Natürlich verfügen die Geräte auch über Access-Listen, die das Management der Geräte selbst schützen.