Akademie
für Lehrerfortbildung
und Personalführung

Sichere Internetanbindung von Schulen

Qualifizierung für Systembetreuer

Teil I
Konzeptionelle Überlegungen

Impressum

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6-7
89407 Dillingen

Autor: Georg Schlagbauer

Beratung und Unterstützung:
Bürgernetz Dillingen
Markus Bader, Staatliche Berufsschule III Fürth
Achim Brunnermeier, Bayerisches Kultusministerium
Wilhelm Drossart, Berufskolleg Neuss
Philipp Flesch, Friedberger Schulnetz
Michael Lotter, Akademie Dillingen
Barbara Maier, Akademie Dillingen

URL: http://alp.dillingen.de/schulnetz
Mail: schlagbauer@alp.dillingen.de
Stand: März 2010

Sichere Internetanbindung von Schulen

Teil I

Konzeptionelle Überlegungen

Inhalt

Vorstellungen von Sicherheit im Schulnetz

Schulnetze existieren in vielfältigen Variationen und sind nach den unterschiedlichsten pädagogischen und technischen Vorstellungen der Schulen gestaltet. Allen gemeinsam ist eine vernetzte Umgebung mit Internetzugang. Durch die Anbindung an das Internet wird von den Schulen erwartet, dass sie sich mit den damit verbundenen Sicherheitsanforderungen auseinander setzen.

Der Begriff „Sicherheit“ wird sehr unterschiedlich definiert. Anbieter von Internetdiensten sehen andere Anforderungen als Benutzer von Internetdiensten. In Verwaltungsumgebungen gelten andere Regeln als in Lernumgebungen. Die Internetnutzung von Kindern und Jugendlichen ist anders zu beaufsichtigen als die Nutzung durch Erwachsene.

Zunächst gilt natürlich auch im Schulnetz, dass das Unterrichtsnetz und vor allem das Verwaltungsnetz vor Angriffen von innen und außen möglichst gut geschützt sein sollen. Ebenso soll die Funktionsfähigkeit der gesamten EDV-Infrastruktur sichergestellt sein. Spezifisch für ein Netz, in dem Schüler arbeiten sind noch zusätzliche Forderungen:

- Schüler sollen im Internet keine Aktionen durchführen können, durch die eventuell Nachteile für die Schüler, die Schule oder die Eltern entstehen könnten.
- Schüler sollen vor nicht geeigneten Inhalten aus dem Internet geschützt werden.

In der Praxis bedeutet dies, dass Schüler z. B. keine Peer-to-Peer-Software für Dateiaustauschdienste oder zum Musik-Download nutzen können sollen oder dass Schüler auf bestimmte Webseiten keinen Zugriff haben sollen. Ebenso sollen z. B. nur die vorgesehene Nutzung des Unterrichtsservers und keine Zugriffe in das Verwaltungsnetz durch Schüler möglich sein.

Um einschätzen zu können, an welcher Stelle Sicherheitsimplementierungen am effektivsten wirken, ist ein grundsätzliches Verständnis der Kommunikation zwischen Computern im lokalen Netz und bei deren Zugriff auf das Internet nötig.

Computer und Netzwerkkomponenten unter dem Aspekt der Sicherheit

Kommunikation zwischen zwei Computern

Jede Kommunikation zwischen zwei Computern funktioniert nach dem Client/Server-Prinzip. Ein Computer bietet einen Dienst an und wartet auf Anfragen. Diesen Computer bzw. diesen Dienst nennt man üblicherweise Server. Korrekter wäre die Bezeichnung Serverprogramm oder Serverdienst, da jeder Computer solche Dienste bzw. Programme ohne eine dedizierte Serverhardware anbieten kann. Bekannte Serverdienste im Internet sind das Web oder E-Mail, im lokalen Netz werden Dateiserverdienste oder Druckdienste häufig genutzt.

Ein Client (besser ein Clientprogramm) greift auf einen Serverdienst zu und dieser antwortet auf die Anfrage. Damit diese Kommunikation funktioniert, muss auf dem Client-PC das zum jeweiligen Serverdienst passende Programm installiert sein. Viele Clientprogramme sind auf jedem PC vorinstalliert (z. B. Webbrowser oder E-Mail-Client).

Abbildung 1: Jede Kommunikation zwischen zwei Computern basiert darauf, dass ein Client über ein Verbindungsnetz auf einen Server zugreift. Das Verbindungsnetz kann z. B. das lokale Netzwerk (LAN) oder auch das Internet sein.

Typische Kommunikationsprozesse in der Schule sind die folgenden:

- Ein Arbeitsplatzcomputer greift auf den Schulserver zu (z. B. auf eine Dateifreigabe).
- Ein Arbeitsplatzcomputer greift auf einen Server im Internet zu (z. B. auf einen Webserver).
- Auf einem Arbeitsplatzcomputer wird ein Serverdienst gestartet, ein anderer Computer greift darauf zu (z. B. Dateiaustausch).

Um ein Netz abzusichern und funktionsfähig zu erhalten, muss unerwünschte Kommunikation verhindert werden. Dazu kann man am Client, am Server oder an den aktiven Netzwerkkomponenten ansetzen.

Im Folgenden sollen die Arbeitsplatzcomputer, die Server in der Schule sowie die dem Verbindungsnetz zugeordneten Geräte wie Switche, Router und Access-Points bezüglich der Möglichkeiten eines steuernden und kontrollierenden Eingriffs näher betrachtet werden.

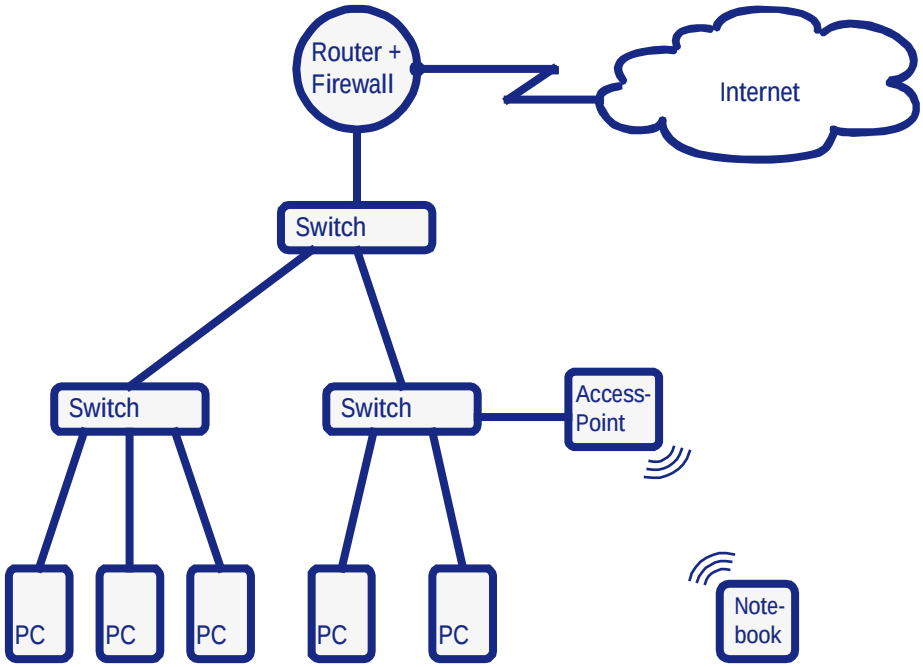


Abbildung 2: Um die Kommunikation zwischen zwei Computern zu beeinflussen, kann an den beteiligten Computern oder an den verbindenden aktiven Netzwerkkomponenten (Router, Switch, Access-Point) eingegriffen werden.

Die Arbeitsplatzcomputer

Bei den Arbeitsplatzcomputern in der Schule steht die Funktionsfähigkeit der Computer im Vordergrund, d. h. Schüler und Lehrkräfte sollen in jeder Unterrichtsstunde einen funktionsfähigen Computer vorfinden. Für die Erhaltung der Funktionsfähigkeit gibt es gute Lösungen. Diese sind z. B. Systemsicherungen, Clonen der PCs, nicht administrativer Benutzerzugang mit entsprechenden Restriktionen oder die Absicherung der Computer durch eine Protektorlösung (Festplattenschutz).

In Firmen- oder Verwaltungsumgebungen versucht man durch eine Kombination aus technischen Restriktionen und entsprechenden Benutzervereinbarungen oder Unternehmensrichtlinien festzulegen, dass die Computer nur in der vorgesehenen Weise und zur Erfüllung der Arbeitsaufgaben genutzt werden dürfen.

In Unterrichtsnetzen stehen andere Aspekte im Vordergrund:

- In einer Lernumgebung sind grundsätzlich mehr Freiheiten notwendig als in einem Firmen- oder Verwaltungsnetz. Restriktive Einstellungen verhindern ein selbstgesteuertes Lernen und behindern dadurch Lernprozesse.
- Der Austausch von Dokumenten zwischen den häuslichen und den schulischen Arbeitsplätzen ist normal und erwünscht. Dadurch können aber auch Schadprogramme transportiert werden.
- Eine eindeutige Zuordnung „Benutzer zu Computer“ ist nicht immer gegeben. Dadurch reduziert sich das Verantwortungsgefühl für den eigenen Arbeitsplatz.
- Belehrungen oder Nutzungsvereinbarungen greifen im Vergleich zur Arbeitswelt nur bedingt. Ebenso fehlen echte Sanktionsmöglichkeiten. Dadurch wächst die Versuchung, unerlaubte Programme zu testen oder gezielt nach Schwachstellen im Netz zu suchen.

- Lehrkräfte und Schüler bringen ihre persönlichen Notebooks in die Schule mit und nutzen die zur Verfügung gestellte Infrastruktur. Der Systembetreuer bzw. die Systembetreuerin der Schule hat keinen administrativen Zugriff auf diese Geräte und hat keinen Einfluss auf die darauf installierten Programme.

Grundsätzlich hat ein Benutzer an einem ihm physikalisch zugänglichen Computer sehr viele Bedien- und Manipulationsmöglichkeiten. Will man die Sicherheit im Schulnetz durch eine Kontrolle der Arbeitsplatzcomputer erreichen, so ist dies nur mit einem relativ hohen Aufwand und mit zweifelhaftem Erfolg möglich. Effektiver ist es, an den zentralen Stellen in einem Netz für Sicherheit zu sorgen.

Der Server in der Schule

Bei einem Server geht man davon aus, dass dieser für die Benutzer physikalisch nicht zugänglich ist. Die Benutzer haben keinen Zutritt zum Serverraum und können nur über die vom Server angebotenen Dienste auf diesen zugreifen.

Die Server müssen nicht jedem Client ungehinderten Zugriff gewähren. Bekannte Methoden der Zugriffsbeschränkung sind beispielsweise die Abfrage von Benutzernamen und Passwort oder die Abfrage eines Sicherheitszertifikats.

Die Sicherheit besteht im Wesentlichen darin, auf dem Server

- nur notwendige Dienste zu aktivieren,
- administrative Zugänge entsprechend abzusichern,
- den Benutzern nur die notwendigen Rechte zu erteilen,
- durch regelmäßige Sicherheitsupdates Angriffen auf bekannt gewordene Schwachstellen vorzubeugen,
- ggf. durch einen Virenscanner die auf dem Server abgelegten Benutzerdaten zu überprüfen
- sowie durch eine regelmäßige Daten- und Systemsicherung einen möglichen Schaden zu begrenzen.

Beliebte Methoden, sich nicht autorisiert Zugang zum Server zu verschaffen, sind Sicherheitslücken in der Berechtigungsstruktur aufzuspüren oder fremde Benutzerzugänge auszuprobieren. Angriffe mit Methoden wie sie aus dem Internet bekannt sind, sind im lokalen Netz kaum zu erwarten. Deshalb ist ein sicherer Betrieb hier vergleichsweise einfach herzustellen.

Ist ein schulischer Server auch aus dem Internet erreichbar, dann ist zur Absicherung und zur Gewährleistung einer ständigen Verfügbarkeit ein höherer administrativer Aufwand erforderlich.

Switche

Switche (genauer gesagt: Layer-2-Switche) sind Netzwerkkomponenten, die dafür ausgelegt sind, den Datenverkehr möglichst schnell und ohne Filterung an das Zielgerät weiterzuleiten. Es gibt zwar Switche, die eine Authentifizierung nach MAC-Adressen oder nach Benutzernamen (802.1X-Protokoll) unterstützen, dabei handelt es sich aber nur um eine grundsätzliche Zugangskontrolle, ohne dass nach bestimmten Anwendungen oder Zieladressen unterschieden wird. Für einen steuernden oder kontrollierenden Eingriff sind Switche damit nur bedingt geeignet.

Managebare Switche ermöglichen es, Netze in verschiedene Teilbereiche (Teilnetze oder VLANs) aufzuteilen und können dadurch z. B. verhindern, dass Störungen in einem Netz auf ein anderes Teilnetz übergreifen. Diese Teilnetze müssen dann jedoch wieder durch einen Router oder einen Layer-3-Switch (mit Routing-Funktionen) zusammengeführt werden.

Access-Points

Access-Points ermöglichen den Zugriff über WLAN und arbeiten auf der gleichen Ebene wie Switche. Die Funkverbindung sollte stets verschlüsselt erfolgen und es sollte nur autorisierten Personen Zugriff gewährt werden. Dies erreicht man mit einer Verschlüsselung über WPA- oder WPA2 und einem vorher vereinbarten Passwort oder bei einer größeren WLAN-Infrastruktur auch nach einer Authentifizierung über einen Authentifizierungsserver (802.1X-Protokoll).

Die Funktion „Multi-SSID“ ermöglicht den differenzierten WLAN-Zugang über einen Access-Point. Damit können z. B. Schüler und Lehrer abhängig von Ihrer Anmeldung auf unterschiedliche Teilnetze (VLANs) zugreifen.

Für weitergehende Sicherheitsimplementierungen sind Access-Points ähnlich wie Switche nur bedingt geeignet.

Layer-3-Switche

Layer-3-Switche werden so genannt, weil sie auch Funktionen von Routern übernehmen können (die auf der Schicht 3 des ISO/OSI-Modells arbeiten). Die Vorteile von Layer-2-Switchen, für einen möglichst schnellen Datenverkehr zu sorgen, sollen dabei erhalten bleiben. Layer-3-Switche werden zunehmend innerhalb eines lokalen Netzes zur Trennung des lokalen Netzes in voneinander geschützte Teilnetze eingesetzt. Ebenso sind damit Sicherheitsimplementierungen möglich, indem durch Filterlisten festgelegt wird, welche Teilnetze aufeinander zugreifen dürfen.

Der Internetzugangsrouter

Der Internetzugangsrouter der Schule ist ein zentraler Übergangsknotenpunkt, an dem man sehr effektiv den Datenfluss zwischen dem lokalen Netz und dem Internet steuern kann. An dieser Stelle wird bestimmt, welcher Datenverkehr das interne Netz verlassen darf und welche Daten in das interne Netz gelangen können. Grundsätzlich kann jedes Datenpaket, das diesen Knotenpunkt passiert, kontrolliert und gegebenenfalls geblockt werden.

Bereits mit einer Standardkonfiguration bieten Internetzugangsrouter einen guten Schutz gegen Angriffe oder ungewollte Zugriffe aus dem Internet. Gleichzeitig lassen sie jedoch jede Datenübertragung zu, die aus dem internen Netz initiiert wird. Sollen diese Möglichkeiten eingeschränkt werden, können mit Filterregeln unerwünschte Dienste und Anwendungen mit einem relativ geringen Aufwand blockiert oder in der Nutzung zumindest erheblich erschwert werden.

Router und Layer-3-Switche bieten sehr viele Möglichkeiten, Verbindungen zu beschränken oder einzurichten. Allerdings gilt dies nicht für jeden preiswerten Internetzugangsrouter oder Layer-3-Switch.

Das lokale Netz

Kommunikation im lokalen Netz

Ein lokales Netz (LAN, Local Area Network) ist ein Netz, dessen Ausdehnung auf ein Gebäude oder auf einen Gebäudekomplex beschränkt ist.

Ein einfaches lokales Netz ist ein Gebilde, in dem mehrere Computer oder andere Netzwerk-Endgeräte über einen oder mehrere Switche (Layer-2-Switche) miteinander verbunden sind. Typisch an einem solchen Netz ist, dass jeder Computer mit jedem anderen Computer kommunizieren kann, ohne dass ein Router als Vermittlungsinstanz dazwischen geschaltet ist. Die Computer finden einander durch Rundrufe (Broadcasts), die von den Switchen an alle Endgeräte weitergeleitet werden.

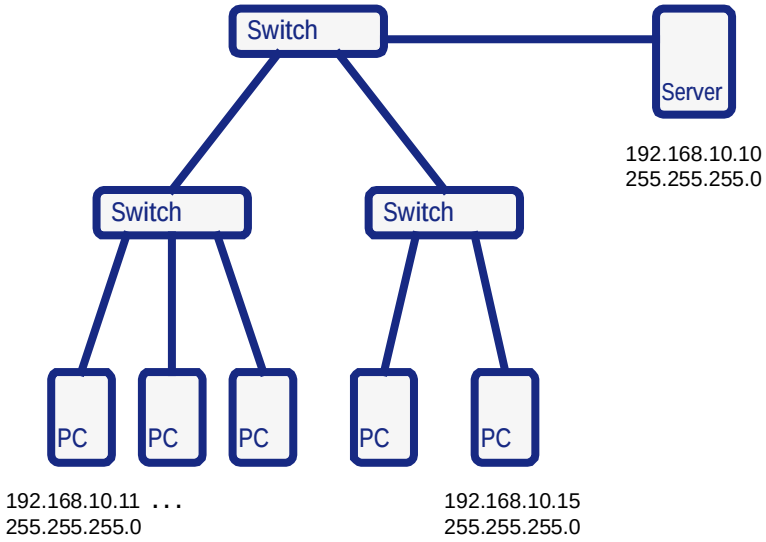


Abbildung 3: Einfaches lokales Netz: Alle Computer sind über Switche verbunden und können sich durch Broadcasts erreichen. Die IP-Adressen aller Computer unterscheiden sich nur durch den Hostanteil (üblicherweise an der letzten Stelle). Der Netzwerkanteil der IP-Adressen und die Subnetzmaske sind bei allen Computern gleich.

Aus der Art und Weise, wie die Computer in einem Netz kommunizieren, lassen sich einige Schlüsse ableiten:

- In einem lokalen Netz sind immer Broadcasts unterwegs. Ein lokales Netz funktioniert nur zuverlässig, wenn sichergestellt ist, dass die Broadcasts an allen Endgeräten ankommen. Unzuverlässige Verbindungen durch schlechte Leitungen, eine schlechte Funkverbindung oder die Auslastung des Netzes bis an die Kapazitätsgrenze führen zu Problemen, die sehr schwer nachvollziehbar und lokalisierbar sind. Die Anzahl der Computer in einem einfachen lokalen Netz sollte deswegen nicht zu groß sein (max. einige hundert PCs). Meist wird jedoch aus den nachfolgend genannten Gründen schon sehr viel früher eine Trennung in verschiedene Netzbereiche vorgenommen.
- Ein einfaches (geswitchtes) lokales Netz ist nicht geeignet, um differenzierte Zugriffsbeschränkungen zwischen zwei oder mehreren Computern auf der Ebene des Netzwerks zu realisieren. Die folgenden Beispiele sollen dies verdeutlichen:

Spontane Kommunikation: Startet ein Schüler oder ein Lehrer an einem PC im lokalen Netz einen Serverdienst (z. B. FTP), so kann jeder im lokalen Netz mit einem entsprechenden Client darauf zugreifen. Viele Lehrkräfte nutzen diese spontanen Netzwerkverbindungen zum Datenaustausch mit den Schülern.

Netzwerkdrucker: Die meisten Netzwerkdrucker verlangen keine Authentifizierung. Wenn Schüler oder Lehrer den entsprechenden Drucker auf ihrem PC installieren, gibt es keine technische Möglichkeit, sie am Drucken zu hindern.

Prüfungsumgebung: Eine eher ungewollte Folge der kommunikativen Struktur im lokalen Netz ist, dass in einem Computerraum mit vertretbarem Aufwand keine Prüfungsumgebung realisiert werden kann, die den Anspruch erfüllt, dass es (allein durch technische Einschränkungen) nicht möglich sein soll, relativ unbemerkt Daten auszutauschen. Derzeit setzen die meisten Realisierungen solcher „Prüfungsumgebungen“ die Aufsicht einer Lehrkraft oder die Unkenntnis der Schüler voraus.

Angriffsmöglichkeiten: Durch die zur Kommunikation notwendigen Broadcasts gibt es grundsätzlich sehr viele Angriffsmöglichkeiten. Diese reichen von der Möglichkeit, ein Netz durch Broadcast-Stürme lahmzulegen bis zu sogenannten „Man in the Middle“-Angriffen, bei denen ein Angreifer sich in eine Verbindung schaltet um z. B. Passwörter auszuspähen.

Trennung von Netzen

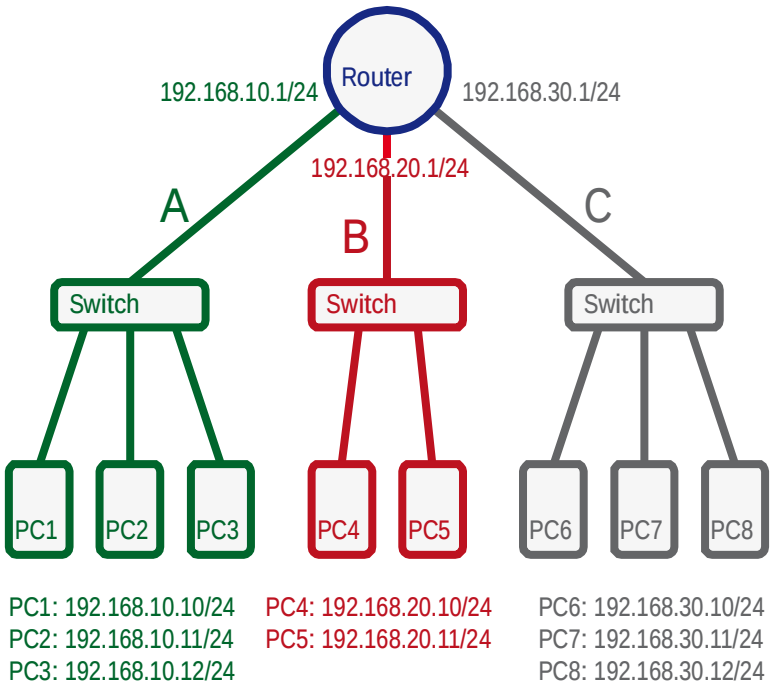


Abbildung 4: Die Grafik zeigt drei getrennte Netze, die über einen Router verbunden sind. Bei den PCs und bei den Router-Schnittstellen sind die IP-Adressen und Subnetzmasken angegeben (/24 ist dabei eine gebräuchliche Abkürzung für die Subnetzmaske 255.255.255.0).

Lokale Netze können in mehrere voneinander geschützte Teilnetze unterteilt werden. Jedes dieser Teilnetze ist ein eigenes Netz (Broadcastdomäne). Die jeweilige Schnittstelle des Routers ist das Standardgateway für die Computer im jeweiligen Netz. Neben der Größe spielen für die Trennung vor allem Sicherheitsaspekte eine Rolle (z. B. Unterrichtsnetz, Verwaltungsnetz).

Die Teilnetze können über einen Router oder einen Layer-3-Switch verbunden werden. Damit kann eine Kommunikation zwischen den Teilnetzen ermöglicht werden. Am zentralen Router, der die Netze verbindet, können Sicherheitsbarrieren (Firewall-Funktionen) eingerichtet werden.

Kommunikation zwischen den Teilnetzen

Zur Verbindung von Teilnetzen ist ein Router oder ein Layer-3-Switch nötig. Damit lassen sich kontrollierbare Übergänge einrichten. An dieser Stelle kann sehr detailliert geregelt werden, wer mit wem über welches Protokoll kommunizieren kann. In der Schule ließe sich zum Beispiel regeln, dass sowohl vom Computerraum, der Bibliothek und dem Lehrerzimmer auf den Schulserver zugegriffen werden kann, ohne dass ein Zugriff vom Computerraum in das Lehrerzimmer möglich ist. Ebenso könnte geregelt werden, dass von einem Computer aus dem Verwaltungsnetz der Zugriff auf das Unterrichtsnetz erlaubt, jedoch jeglicher Zugriff vom Unterrichtsnetz in das Verwaltungsnetz verboten ist.

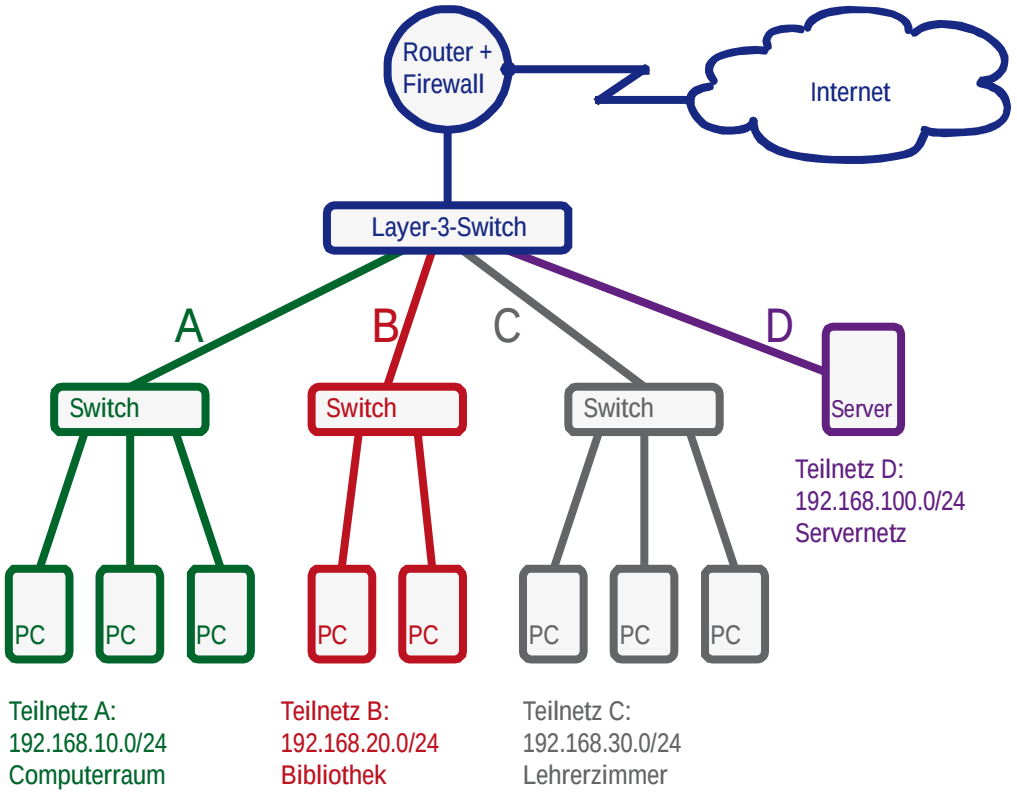


Abbildung 5: Beispielkonfiguration einer größeren Schule mit mehreren getrennten Teilnetzen und eigenem Servernetz. Am Layer-3-Switch wird das lokale Netz in die Teilnetze A, B, C, D getrennt. Der Layer-3-Switch regelt, welche Teilnetze aufeinander zugreifen dürfen. (In der Skizze sind die Netzwerkadressen der Teilnetze angegeben, nicht die IP-Adressen der einzelnen Computer.)

Die Konfiguration von Firewallregeln auf Routern oder Layer-3-Switchen setzt gute Netzwerkkenntnisse voraus. Nach dem Anschluss der Teilnetze und einer Erstkonfiguration sind die Router zunächst einmal auf „Kommunikation“ ausgerichtet. Die steuernden Firewallregeln müssen explizit gesetzt werden. Der Layer-3-Switch in Abbildung 5 könnte beispielsweise so konfiguriert sein, dass die einzelnen Teilnetze in das Servernetz und auf das Internet zugreifen können; eine Verbindung zwischen den einzelnen Teilnetzen ist nicht erlaubt.

Layer-3-Switche ermöglichen einen höheren Datendurchsatz (z. B. Gigabit-Ethernet) als Router, die Firewallregeln lassen sich dagegen bei einem Router in der Regel differenzierter gestalten.

VLANs (Virtuelle LANs)

In Abbildung 5 konnte jeder Port des Layer-3-Switch genau einem Teilnetz zugeordnet werden. Nun kann es aber in der Praxis vorkommen, dass beispielsweise das Bibliotheksnetz oder die Lehrerzimmer auf mehrere Etagen oder Gebäude verteilt sind, die Trennung der Netze also nicht mit der räumlichen Trennung übereinstimmt.

In diesem Fall bietet sich die Trennung des Netzes durch VLANs an. Dabei erfolgt die Zuordnung eines Computers in ein VLAN durch die Konfiguration der nachgeordneten Switche. Jedem Port des Switch wird ein VLAN zugeordnet (port-basiertes oder statisches VLAN). Die Verbindung der Switche und Router erfolgt über sogenannte Trunk-Leitungen. Die Datenpakete, die über diese Trunk-Leitungen geschickt werden sind mit ihrer jeweiligen VLAN-Markierung gekennzeichnet (tagging), damit sie den einzelnen VLANS zugeordnet werden können.

Die Konfiguration von VLANs setzt wie die Konfiguration von Routern oder Layer-3-Switchen gute Netzwerkkenntnisse voraus.

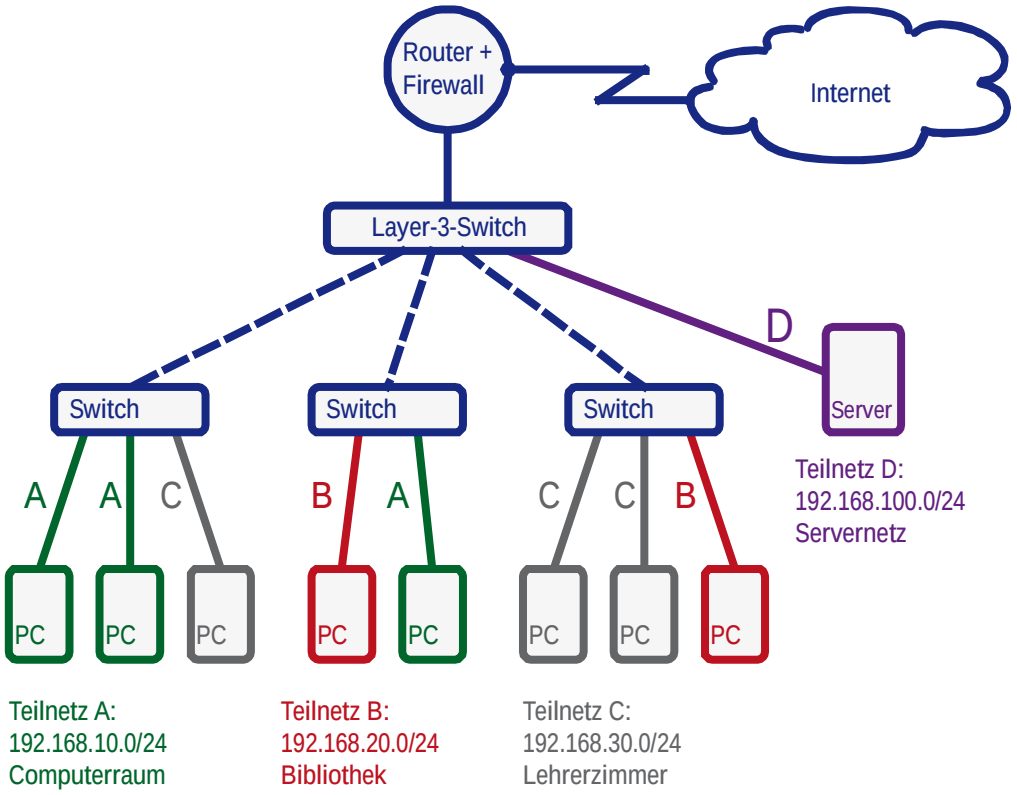


Abbildung 6: In der Grafik ist das lokale Netz in VLANs (A, B, C, D) unterteilt. Die unterbrochen gezeichneten Linien sind Trunk-Leitungen.

Eine direkte Kommunikation ist nur zwischen Geräten im gleichen VLAN möglich. Die Kommunikation zwischen Geräten aus verschiedenen VLANs ist über einen Layer-3-Switch oder einen Router möglich, falls dies nicht durch Firewallregeln unterbunden wird. Geht man davon aus, dass die VLAN-fähigen Switche richtig konfiguriert und entsprechend abgesichert sind, bietet die logische Trennung eines Netzes durch port-

basierte VLANs die gleiche Sicherheit wie eine echte Trennung der verschiedenen Netze.

Mit VLANs hat man damit ein Konzept, mit dem jeder PC ohne Änderung der Verkabelung einem bestimmten Netz zugeordnet werden kann. Zu beachten ist, dass die Trunk-Leitungen und Uplink-Leitungen, über die der gesamte Datenverkehr läuft, eine entsprechende Bandbreite benötigen.

Physikalisch getrennte Netze – Versuch einer Definition

Die Unterteilung eines lokalen Netzes in Teilnetze ist ab einer bestimmten Größe der Netze oder aber auch aus Sicherheitsüberlegungen sinnvoll. In der Schule empfehlen manche Schulträger eine „physikalische Trennung“ von Unterrichtsnetz und Verwaltungsnetz, wobei der Begriff der „physikalischen Trennung“ aus einer Zeit stammt, als man noch nicht an den Internetanschluss der Schulen dachte und die Trennung eines lokalen Netzes in voneinander geschützte Teilnetze weitgehend unbekannt war.

Sowohl das Unterrichtsnetz als auch das Verwaltungsnetz einer Schule sind heute an das Internet angeschlossen und damit letztendlich auch miteinander verbunden. Techniken, wie sie bei virtuellen Netzwerken (z. B. Skype, Teamviewer, Hamachi) verwendet werden, ermöglichen die direkte Kommunikation dieser Netzbereiche über das Internet. Auf der anderen Seite ist es ebenso möglich, dass zwei Teilnetze einen gemeinsamen Internetanschluss nutzen (siehe Abbildung Seite 27) und dennoch keine Kommunikation zwischen diesen Teilnetzen möglich ist – also eine perfekte Trennung.

Dennoch gibt es einen Unterschied:

Bei getrennten Internetzugängen für Unterrichts- und Verwaltungsnetz müsste eine Verbindung bewusst eingerichtet werden, bei einem gemeinsamen Internetzugang könnte eine Verbindung auch durch Nachlässigkeit bei der Konfiguration des verbindenden Routers entstehen.

Als Definitionsversuch zur Diskussionsgrundlage könnte dienen:

Eine physikalische Trennung von zwei Netzen liegt vor, wenn eine mögliche Kommunikation zwischen diesen Netzen nur über ein Netz außerhalb des eigenen administrativen Bereiches (z. B. Internet) möglich ist.

Eine physikalische Trennung von zwei Netzen liegt nach dieser Definition meist nur dann vor, wenn jedes Netz über einen separaten Internetzugang verfügt.

Physikalisch getrennte Netze – Für und Wider

Bei der physikalischen Trennung von Unterrichts- und Verwaltungsnetz ist der Zugriffsschutz von einem Netzbereich auf den anderen bei einer Standardkonfiguration schon gegeben. Verbindungen zwischen den beiden Netzen müssten zumindest bewusst hergestellt werden.

In der Praxis kommt es häufig vor, dass trotz der gewollten Trennung von Unterrichts- und Verwaltungsnetz bestimmte Ressourcen aus beiden Netzen gemeinsam genutzt werden sollen. Mögliche Beispiele sind:

- Ein spezieller Drucker soll sowohl im Verwaltungs- wie im Unterrichtsnetz genutzt werden.
- Die Lehrkräfte in der Schulverwaltung (Schulleitung, etc.) sollen von ihrem Arbeitsplatzcomputer aus (Verwaltungsnetz) Daten auf dem Server im Unterrichtsnetz ablegen können.

- Die tägliche Datensicherung erfolgt auf einem eigenen Backupserver. Dieser soll den Verwaltungsserver und den Unterrichtsserver sichern.

Bei einer strikten physikalischen Trennung der Netze ist eine gemeinsame Nutzung von Ressourcen nicht oder nur mit erhöhtem Aufwand möglich.

Persönliche Notebooks im Schulnetz

Aus der Sicht eines Systemadministrators, der für die Sicherheit in seinem Netzwerk verantwortlich ist, präsentieren sich persönliche Notebooks von Lehrern und Schülern immer als „Fremdkörper“, auf die er keinen Einfluss hat und die er deshalb gerne verbieten würde.

Hat der Systemadministrator jedoch sein (übriges) Netzwerk im Griff und durch geeignete Maßnahmen dafür gesorgt, dass sich mögliche Schadprogramme von einem Notebook aus nicht in seinem Netz ausbreiten können, so eröffnen sich neue Betrachtungsweisen: Die persönlichen Notebooks von Lehrkräften und Schülern entlasten die Schule. So könnte es genügen, dass die Schule nur noch die Vernetzung und zentrale Ressourcen zur Verfügung stellt und den Schülern und Lehrern die Möglichkeit einräumt, ihre mobilen Geräte in das Netzwerk der Schule zu integrieren.

Die Benutzer müssen selbst für einen ausreichenden Schutz ihrer mobilen Geräte sorgen. Bringt man sein persönliches Notebook in ein fremdes Netz (z. B. in einem Hotel, an einem Hotspot oder auch in der Schule), kann man natürlich nie sicher sein, dass in diesem Netz keine Viren oder andere Schadprogramme kursieren oder dass im Extremfall sogar gezielt versucht wird, auf das Notebook über das Netzwerk zuzugreifen. Da das Notebook anders als ein Server keine Dienste bereitstellen muss, ist ein Schutz gegen Fremdzugriff oder gegen Viren relativ leicht möglich. Dieser Schutz lässt sich erreichen durch

- sichere Passwörter,
- regelmäßige Installation der Sicherheitsupdates,
- einen aktueller Virenscanner,
- Einschalten der windowseigenen Firewall (ohne Ausnahmen).

Aus den letzten Jahren ist kein Schadprogramm bekannt, das in der Lage gewesen wäre, diesen Schutz zu überwinden.

Anwendungen und Dienste im Internet

Im engeren Sinne stellt das Internet selbst lediglich eine Infrastruktur bereit. Es bestimmt, wie Daten von einem Ort zu einem anderen Ort übertragen werden. Die im Internet angebotenen Dienste oder Anwendungen nutzen diese Infrastruktur.

Die bekanntesten Anwendungen im Internet sind das World Wide Web (WWW) und E-Mail.

Web

Das World Wide Web dient zur Übertragung von Webseiten, die in HTML (Hypertext Markup Language) erstellt sind. Die Webseiten werden in einem Browser dargestellt, als Übertragungsprotokoll dient http oder bei einer verschlüsselten Übertragung https. In die Browser wurden immer mehr Funktionen integriert, um die Möglichkeiten des Web zu erweitern. So werden zunehmend Anwendungen, für die früher eigene Dienste nötig waren, über das http-Protokoll übertragen und im Browser dargestellt (z. B. Download von Dateien, E-Mail, Darstellung von Bildern, Animationen, Videos, Internetradio, Chat). Viele dieser im Browser integrierten Anwendungen haben jedoch nicht die volle Funktionalität.

E-Mail

Zum Versenden von E-Mail dient das SMTP-Protokoll (Simple Mail Transfer Protocol). Zum Empfang von E-Mails gibt es die Protokolle POP3 (Post Office Protocol) oder IMAP (Internet Message Access Protocol). Während bei POP3 die einkommenden E-Mails auf den jeweiligen PC verschoben oder kopiert werden, verbleiben bei IMAP die E-Mails auf dem Server. Zunehmend wird der E-Mail-Dienst den Endanwendern auch über das http- bzw. https-Protokoll zur Darstellung in einem Webbrowser angeboten (Web-Mail).

FTP

FTP steht für File Transfer Protokoll und ist ein sehr einfaches und schnelles Protokoll zum Kopieren von Dateien über das Internet oder in einem lokalen Netz. In den letzten Jahren ist FTP etwas in Verruf gekommen, da alle Daten (auch Passwörter) im Klartext übertragen werden und somit prinzipiell von jedem gelesen werden könnten, der irgendwo auf dem Übertragungsweg „mithören“ kann.

Für E-Mail und FTP gibt es auch Protokolle, die eine verschlüsselte Übertragung ermöglichen. Diese sind jedoch noch wenig verbreitet.

Tauschbörsen

Tauschbörsen zum Online-Tausch von Musik oder Videofilmen nutzen heute gerne Peer-to-Peer-Verbindungen. Dabei ist jeder beteiligte Computer sowohl Anbieter wie auch Abnehmer. Um hohe Download-Raten zu erreichen, muss man die herunter geladenen Dateien anderen Nutzern ebenfalls zum Download anbieten, das heißt, der Computer sollte aus dem Internet erreichbar sein. Steht ein lokaler Computer hinter einer Firewall, so ist dies nicht immer der Fall. Die meisten Peer-to-Peer-Verbindungen funktionieren zwar trotzdem, jedoch mit sehr unattraktiv niedrigen Download-Raten.

Chat und Instant Messaging

Die Grundidee dieser Programme ist, dass man am eigenen Computer sieht, welche seiner Freunde ebenfalls online sind. Mit diesen Personen können quasi live Kurznachrichten ausgetauscht werden. Auf jedem beteiligten PC wird dazu eine Client-Software installiert, die, sobald sie gestartet ist, eine Verbindung zu einem zentralen Server aufbaut und diese Verbindung ständig hält. Dadurch erkennt der zentrale Server, wer gerade online ist und kann dies anderen Anwendern mitteilen oder Nachrichten entsprechend weiterleiten.

Online-Rollenspiele und virtuelle Welten

Ein zentraler Server stellt eine virtuelle Umgebung bereit. Die einzelnen Mitspieler loggen sich dort ein und spielen mit. Bekannt sind Kampfspiele, meist Ego-Shooter oder virtuelle Welten wie World of Warcraft oder Second Life, bei denen sich die Mitspieler in einer Scheinwelt bewegen.

Virtuelle Netzwerke

Mit Tools wie Hamachi, Teamviewer, Skype und vielen anderen werden private Netzwerke über das Internet aufgebaut. Technisch funktioniert dies so, dass auf jedem beteiligten PC ein Client installiert ist, der eine ständige Verbindung zu einem Vermittlungsserver im Internet aufrecht hält. Dieser Vermittlungsserver schaltet dann die Clients zusammen, damit diese kommunizieren können.

VPN steht für Virtual Private Network und bedeutet, dass sich jemand mit einer verschlüsselten Verbindung von seinem Computer aus in ein anderes Netz verbindet. Über eine VPN-Verbindung könnte ein Lehrer am Computer zu Hause so agieren, als wäre der Computer im Schulnetz. Sehr häufig werden VPN-Verbindungen zur Remote-Administration von Computern oder zur Remoteunterstützung von Benutzern eingerichtet. In einem solchen Fall hat ein „Hilfesuchender“ z. B. ein Icon auf seinem Desktop. Wenn er dieses anklickt, wird automatisch eine VPN-Verbindung zu einem Service-Leistenden aufgebaut, der den Computer des Hilfesuchenden fernsteuern kann.

Die Anbindung an das Internet

Schulen sind heute normalerweise über DSL an das Internet angeschlossen. Die Internetanbindung wird dabei über einen DSL-Router hergestellt. Dieser verbindet das lokale Netz mit dem Internet.

Beim Verbindungsaufbau erhält der DSL-Router vom Provider eine temporär vergebene (dynamische) öffentliche IP-Adresse. Die Verwendung statischer öffentlicher Adressen ist eher selten, aber möglich. Über diese öffentliche IP-Adresse ist der DSL-Router aus dem Internet erreichbar. Die PCs im lokalen Netz haben eine private IP-Adresse und sind somit aus dem Internet heraus nicht direkt ansprechbar.

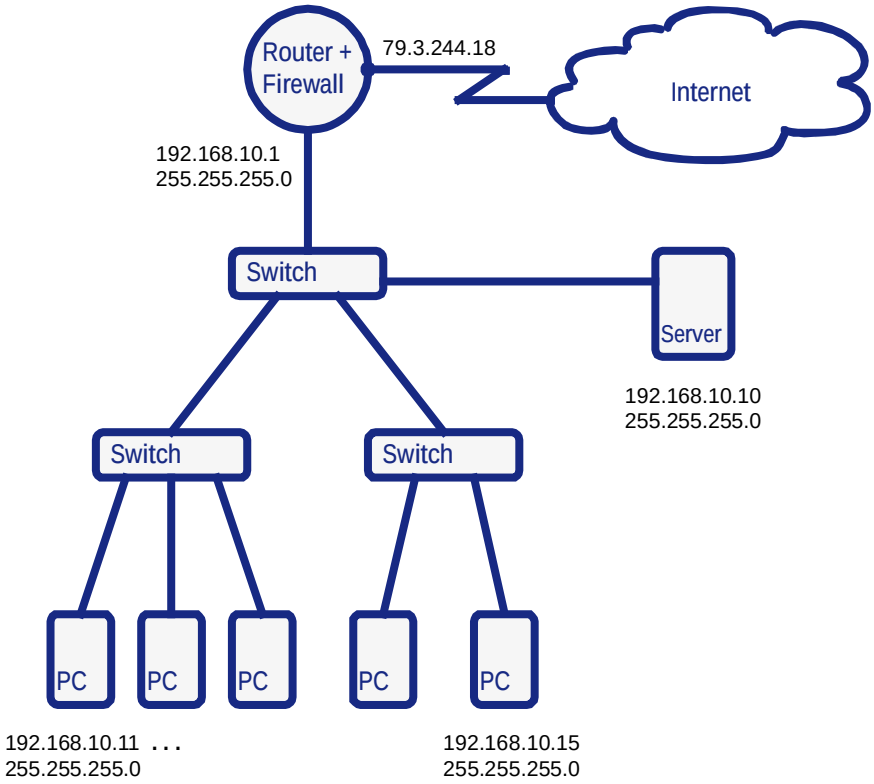


Abbildung 7: Öffentliche und private IP-Adressen; nur die externe Schnittstelle des Routers hat eine öffentliche IP-Adresse und ist aus dem Internet erreichbar.

Damit Computer im lokalen Netz auch mit Computern im Internet kommunizieren können, versieht der Router alle Pakete, die das lokale Netz verlassen, mit seiner eigenen öffentlichen IP-Adresse (Netzadressübersetzung).

Durch die Netzadressübersetzung (NAT) bieten Internetzugangsrouter (z. B. DSL-Router) einen guten Schutz gegen Angriffe aus dem Internet. Bei Zugriffen von innen sind standardmäßig keine Beschränkungen gesetzt, die Router lassen alles zu, was aus dem internen Netz initiiert wird.

Auch bei einer anderen Art der Anbindung einer Schule (z. B. über Kabelmodem oder Standleitung) ändert sich der grundlegende Aufbau nicht. Ein Router, der oft auch als Gateway bezeichnet wird, stellt die Verbindung zum Internet her. Die Computer im lokalen Netz sind aufgrund ihrer privaten IP-Adressen von außen nicht direkt erreichbar.

Grundsätzlich bieten Router sehr viel weitergehende Möglichkeiten, Verbindungen zu beschränken oder einzurichten, auch wenn nicht alle Möglichkeiten bei jedem preiswerten DSL-Router konfigurierbar sind.

Firewall bei Zugriffsversuchen von außen

Obwohl durch die Netzadressübersetzung bereits ein guter Schutz gegen Zugriffe von außen gegeben ist, setzen viele Router zusätzlich auf eine Firewall, die überprüft, ob ein von außen ankommendes Paket zu einer Verbindung passt, die von innen initiiert wurde. Stellt die Firewall fest, dass dies nicht der Fall ist, wird ein von außen ankommendes Paket verworfen (Stateful Inspection Firewall).

Port-Weiterleitung

Um gezielt Verbindungen von außen zuzulassen (z. B. beim Betrieb eines öffentlich zugänglichen Webservers oder zur Fernadministration eines Servers), werden Zugriffe von außen auf bestimmte Ports der Zielrechner im internen Netz weitergeleitet.

Server, die von außen erreichbar sind, sind prinzipiell auch von außen angreifbar. Angriffe aus dem Internet erfolgen dabei üblicherweise, indem bekannt gewordene Sicherheitslücken der Serverdienste ausgenutzt werden oder durch ein automatisiertes Probieren von mehreren Tausend Benutzernamen- und Passwort-Kombinationen.

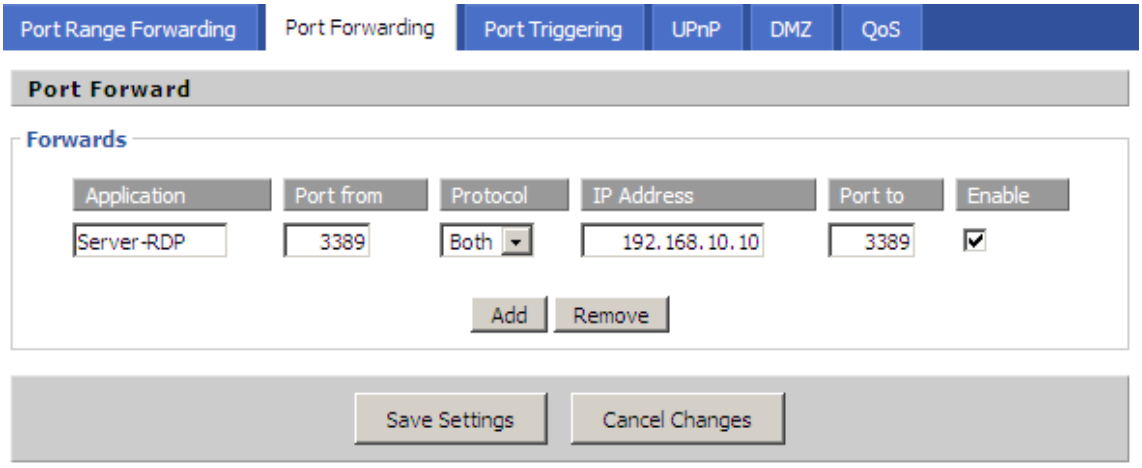


Abbildung 8: Beispielkonfiguration für eine Portweiterleitung, um per Remotedesktop (Port 3389) auf einen Rechner im schulischen Netz (192.168.10.10) zugreifen zu können.

VPN-Verbindungen

Viele Router erlauben das Einrichten von VPN-Verbindungen (Virtual Private Network). Damit kann man sich z. B. von zu Hause aus über eine verschlüsselte Internetverbindung in das Netz der Schule einwählen und hat damit die gleichen Möglichkeiten wie im internen lokalen Netz der Schule.

Beschränkungen bei Zugriffen von innen

Standardmäßig ist der Zugriff auf das Internet nicht eingeschränkt. Ein Router ist jedoch in der Lage, gezielt Beschränkungen zu setzen. So können beispielsweise bestimmte Peer-to-Peer-Verbindungen wie diverse Chat oder Tauschbörsen gesperrt oder die Internetzugriffe auf Webverbindungen (http) beschränkt werden. In begrenztem Umfang bieten einige DSL-Router auch eine Webfilterung an, um Inhalte bzw. Seiten zu sperren.

Anwendungen und Dienste im Internet und im lokalen Netz verwenden eindeutige Protokolle, über die sie auch identifizierbar sind. Traditionell sind diese Protokolle an bestimmte Protokollports am Server gebunden. Der Server „lauscht“ auf diesen Ports auf die Anfragen der einzelnen Clients. Am bekanntesten ist der Port 80, auf dem die Webserver im Internet auf die Anfragen der Webbrowser reagieren. Router sind über Filterregeln in der Lage, bestimmte Ports und damit die Anwendungen in die jeweiligen Zielnetzwerke (z. B. das Internet) freizugeben oder zu blockieren. Wenn in einem Netzwerk auf Sicherheitseinstellungen geachtet wird, sind deshalb nur Ports zu benötigten Anwendungen im Internet offen.

In den letzten Jahren versuchen immer mehr Anwendungen (insbesondere Tauschbörsen und Virtuelle Netzwerke) den Nutzern einen Weg durch restriktiv administrierte Netzwerke zu ermöglichen, indem sie das Netzwerk nach freien Ports ins Internet scannen und dann erst eine Verbindung aufbauen. Um dies zu erkennen, müsste eine Firewall neben den verwendeten Ports auch noch das zugehörige Protokoll überprüfen (z. B. http bei Port 80). Dies wird von gängigen Firewall-Routern derzeit nicht abgedeckt und ist den sogenannten Proxys vorbehalten.

Eine andere Variante, Beschränkungen zu umgehen, bieten Webanwendungen. Zunehmend lassen E-Mail-Server – oder auch Chat- und Messaging-Programme – Webbrowser gestützte Verbindungen (über das http-Protokoll auf Port 80) zu. Der Webdienst kann üblicherweise nicht blockiert werden, da sonst alle Webangebote blockiert würden. Eine differenzierte Sperre oder Freigabe einzelner Webangebote funktioniert üblicherweise mit einem Proxy und einer Webfilterung.

In der Praxis ist es derzeit dennoch relativ gut möglich über Firewallregeln, gegebenenfalls in Verbindung mit Proxys, nicht gewünschte Anwendungen zu blockieren oder deren Nutzung so zu erschweren, dass diese uninteressant werden.

Proxys

Übliche Firewalls arbeiten auf IP-Adress- und Port-Ebene (Schichten 3 und 4 im ISO/OSI-Referenzmodell) und sind in der Lage bestimmte Anwendungen differenziert nach Absende- oder Zieladresse zu blockieren oder zuzulassen. Weiter differenzierende Kriterien sind bei Proxys möglich.

Ein Proxy (Stellvertreter) ist ein Serverdienst, der auf der Anwendungsebene (Schicht 7 im ISO/OSI-Referenzmodell) arbeitet. Proxys gibt es für verschiedene Internet-Anwendungen, z. B. für http, ftp, smtp. Am bekanntesten sind die Web-Proxy (z. B. Squid). Ein Client baut dabei keine direkte Verbindung zum Internet auf, sondern sen-

det seine Anfrage an den Proxy. Dieser sendet daraufhin eine eigenständige Anfrage an den Webserver und leitet die Antwort an den Client weiter. Der Webserver im Internet sieht als Absender nur den Proxy und nicht den anfragenden Client.

Zwischenspeicher

Ein Proxy kann die Inhalte auch zwischenspeichern, so dass Anfragen verschiedener Clients an die gleiche Webadresse nur einmal vom Zielrechner im Internet angefordert werden müssen. Dieser Geschwindigkeitsvorteil kann allerdings nur bei statischen Webseiten zum Tragen kommen.

Sicherheitsfunktion

Da ein Client Anfragen über den Proxy leitet, hat der Proxy auch eine Sicherheitsfunktion. Mögliche Angriffe aus dem externen Netz sind zunächst an den Proxy gerichtet und treffen nicht den Client.

Bei einer Anfrage eines Clients wartet ein Proxy die gesamte Antwort vom Zielrechner ab und sendet diese erst dann an den Client, wenn sie vollständig angekommen ist. Ein Proxy kennt damit den vollständigen Inhalt der angefragten Information und kann diesen analysieren (z. B. Inhaltsfilter, Virenscanner, ...).

Benutzerauthentifizierung

Ein Proxy kann eine Benutzerauthentifizierung verlangen. In diesem Fall müssen beim Öffnen eines Webbrowsers Benutzername und Passwort eingegeben werden. Die Webzugriffe können auch protokolliert werden. Dabei sind jedoch die Datenschutzbestimmungen zu beachten.

Ein Proxy kann differenziert nach Uhrzeit, Absender-IP und Benutzernamen einen Webzugriff erlauben oder verweigern. Diese Funktionalität wird auch bei Webfiltern genutzt. Damit ließe sich beispielsweise ein uneingeschränkter Webzugang im Lehrerzimmer realisieren, während der Internetzugang im Klassenzimmer restriktiver geregelt ist.

Webfilter

Mit Hilfe eines Proxy lassen sich Webadressen (URLs) und Nutzdaten einer Verbindung auswerten. Einsatzgebiete eines Webfilters können sein:

- Herausfiltern von Webseiten, die ActiveX, Java oder JavaScript-Elemente enthalten,
- Überprüfung von Downloads nach Viren oder anderen Schadprogrammen,
- Unterbindung des Downloads bestimmter Dateitypen,
- Sperren unerwünschter Webseiten anhand von Schlüsselwörtern oder Filterlisten.

Der letzte Punkt ist vor allem für Schulen interessant. Dazu werden vielfältige Produkte angeboten.

URL-Filterlisten

Die meisten angebotenen Webfilter arbeiten mit URL-Filterlisten. Die Anbieter versuchen dabei möglichst alle Webseiten zu erfassen und jede Webseite einer oder mehrerer Kategorien zuzuordnen (z. B. Spiele, Gewalt, Bildung, …). Dem Filter wird dann mitgeteilt, welche Kategorien geblockt werden sollen. Die angebotenen Filterlösungen lassen es zum Teil auch zu, dass benutzer-, klassenraum- oder zeitspezifisch unterschiedliche Kategorien gesperrt werden.

Von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) wird eine Filterliste (Blacklist) angeboten, die als BPjM-Modul in allen kommerziellen Filterangeboten von

deutschen Anbietern enthalten ist. Die Filterliste enthält ca. 2000 Adressen und sperrt ausschließlich indizierte jugendgefährdende Online-Angebote. Ein wirksamer Kinder- und Jugendschutz ist mit dieser Liste allein nicht gegeben. Selbst frei erhältliche Filterlisten haben in den einschlägigen Kategorien mehrere Millionen Einträge.

Die Filterlisten werden dabei lokal auf dem Proxy vorrätig gehalten und regelmäßig aktualisiert oder es wird bei jeder Webanfrage zunächst ein Filter-Server im Internet nach der zu kategorisierenden Seite befragt.

Der Zielvorstellung, dass möglichst alle Webseiten kategorisiert sind, können die Filterlisten nicht nachkommen. In der Praxis muss deshalb angegeben werden, wie mit den nicht kategorisierten Webseiten verfahren wird. Diese können entweder grundsätzlich geblockt oder freigegeben werden.

Die Qualität eines URL-Filters richtet sich danach, wie viele der angewählten Seiten tatsächlich erfasst sind und wie gut die Kategorisierung dieser Seiten ist. Eine objektive Messung der Qualität eines Filters ist schwierig, da dies immer vom Surf-Verhalten der jeweiligen Zielgruppe abhängt.

Neben kommerziell angebotenen Webfiltern gibt es auch freie Filterlisten für die unterschiedlichsten Kategorien, die in Verbindung mit einem Proxy eingesetzt werden können. Diese freien Filterlisten sind jedoch meist nicht so umfangreich und gut gepflegt wie kommerziell angebotene Lösungen.

Inhaltsfilter

Inhaltsfilter analysieren beim Aufruf einer Webseite die Webadresse, den Dateityp sowie den Inhalt und versuchen die Webseite einer bestimmten Kategorie zuzuordnen. Dabei können prinzipiell auch komplexe Bild- und Textanalyseverfahren zum Einsatz kommen, die jedoch sehr ressourcenintensiv sind und deshalb eher zur Aufbereitung von URL-Filterlisten und nicht für eine Live-Überprüfung verwendet werden.

Für eine inhaltliche Echtzeitüberprüfung von Webseiten eignen sich bisher einfachere Verfahren, die z. B. Webseiten mit bestimmten Schlüsselwörtern sperren oder kritische Wörter mit einer Punktezahl belegen. Wird eine festzulegende Gesamtpunktzahl überschritten, so wird die Webseite für den Benutzer gesperrt.

Online-Abfragen

Einige DSL-Router bieten sehr einfach zu handhabende Filterlösungen mit an. Diese Router nehmen keine Inhaltsfilterung von Webseiten vor und speichern auch keine Filterlisten, sondern fragen bei jeder Webverbindung bei einem Server nach, zu welcher Kategorie eine Seite gehört. Die zu sperrenden Kategorien lassen sich dabei meist nur für alle Anwender gemeinsam statisch einstellen. Der Vorteil dieser Lösung ist, dass ein einziger kleiner Router mit sehr geringem Energieverbrauch alle für die Schule notwendigen Firewall- und Filtereinstellungen – einschließlich eines getrennten Zugangs für die Schulverwaltung – abdeckt. Für kleinere Schulen – oder wenn keine weitere Differenzierung innerhalb der Schule notwendig ist – ist dies ein ausreichender Grundschutz.

DNS-Filter

Eine ebenfalls einfach zu handhabende Filterlösung läuft über bestimmte DNS-Dienstanbieter. Der DNS-Dienst (Domain Name Service) ist notwendig, um die Webadresse (URL) in eine IP-Adresse aufzulösen. Die Schule kann auf der Webseite des Anbieters die zu sperrenden Kategorien auswählen. Bei einer DNS-Anfrage der Schule wird für eine zu blockierende URL eine Webseite zurückgeliefert, die auf die Sperrung hinweist. Eine Differenzierung innerhalb der Schule ist mit diesem Verfahren nicht möglich. Das Verfahren könnte für einfache Webseiten ohne weiterführende Links um-

gangen werden, wenn die korrekte IP-Adresse der gesperrten Seite bekannt ist. In der Praxis kann es dennoch einen ausreichenden Grundschutz für eine Schule bieten.

Virenschutz

Viren und andere Schadprogramme sind ein Ärgernis, das man versuchen sollte, ohne allzu großen Aufwand und möglichst ohne Einschränkung der Arbeitsweise in den Griff zu bekommen. Im Unterrichtsnetz der Schule wäre es beispielsweise eine überzogene Reaktion, wegen der Angst vor Viren den Austausch von Dokumenten zwischen der häuslichen und der schulischen Arbeitsumgebung oder die Verwendung von USB-Sticks oder persönlichen Notebooks zu untersagen. Natürlich kann man nie ausschließen, dass ein mitgebrachter USB-Stick oder ein Notebook einen Virus enthält; deshalb sollte man dafür sorgen, dass sich Viren im Schulnetz nicht ausbreiten können.

Auf den Arbeitsplatzcomputern gibt es dazu zwei grundsätzliche Ansätze, die ggf. auch kombiniert werden können:

- Auf jedem Arbeitsplatzcomputer ist ein Virenscanner installiert, der von einem zentralen Server innerhalb der Schule regelmäßige Updates bezieht. Zusätzlich sollten die Arbeitsplatzcomputer regelmäßige Sicherheitsupdates (z. B. Windows Updates) beziehen, um bekannt gewordene Sicherheitslücken zu schließen.
- Die Arbeitsplatzcomputer der Schule sind mit einer Protektorlösung ausgestattet, die nach jedem Neustart den Computer in einen definierten Ausgangszustand versetzt. Zusätzlich sollte der Arbeitsplatzcomputer zu Beginn oder am Ende der Unterrichtsstunde neu gestartet werden.

Eine ergänzende sehr effektive Möglichkeit, die Übertragung eines Schadprogramms auf einen (Windows-) Client zu verhindern, ist die Aktivierung der Windows-Firewall – nach Möglichkeit ohne Ausnahmen. Dabei ist zu beachten, dass dies auch jede Art von Remotezugriff (z. B. Dunkelschalten der Schülermonitore oder zentrales Herunterfahren der Arbeitsplatzcomputer) verhindert. Gegebenenfalls sind entsprechende Ausnahmen in der Windows-Firewall einzupflegen.

Falls Schüler und Lehrkräfte die Möglichkeit haben, auf einem Dateiserver Daten abzulegen, empfiehlt es sich, die entsprechenden Daten auf dem Dateiserver nach möglichen Viren zu scannen. Am wirkungsvollsten ist ein Livescan der Dateien, in dem Moment, in dem diese Dateien auf dem Dateiserver abgelegt werden. Dies kostet jedoch Leistungsressourcen und verlangsamt den Zugriff. Zumindest sollten die abgelegten Benutzerdateien einmal pro Tag, am besten nachts, auf Viren überprüft werden.

Umgang mit vertraulichen Daten

Die meisten Unsicherheiten entstehen, wenn Benutzer zu sorglos mit vertraulichen Daten umgehen. Zunächst sollte es selbstverständlich sein, dass man nicht unter „Beobachtung“ von anderen Personen Authentifizierungsdaten an einem Computer eingibt.

Wenn man an einem nicht vertrauenswürdigen Computer arbeitet, besteht prinzipiell immer die Gefahr, dass im Hintergrund ein Keylogger-Programm jede Tastatureingabe aufzeichnet und in einer Logdatei speichert. Es gibt auch Trojaner, die entsprechende Benutzereingaben aufzeichnen und über das Internet an einen Zielrechner versenden. Die einzige zuverlässige Möglichkeit sich davor zu schützen ist, an einem nicht vertrauenswürdigen Computer keine vertraulichen Daten zu bearbeiten.

Wenn man vertrauliche Daten im Netzwerk oder auf Datenträgern (z. B. USB-Stick) abspeichert, auf die eventuell auch andere Personen Zugriff erlangen könnten, bietet

es sich an, diese Daten nur verschlüsselt abzuspeichern. Details hierzu sind in der Broschüre „Truecrypt – Datenverschlüsselung in der Schule" (http://alp.dillingen.de/schulnetz/materialien/Truecrypt.pdf) dargestellt.

Ebenso sollten die Daten auch bei der Übertragung über unsichere Netze verschlüsselt werden. Dies gilt insbesondere für die E-Mail-Kommunikation mit vertraulichen Informationen.

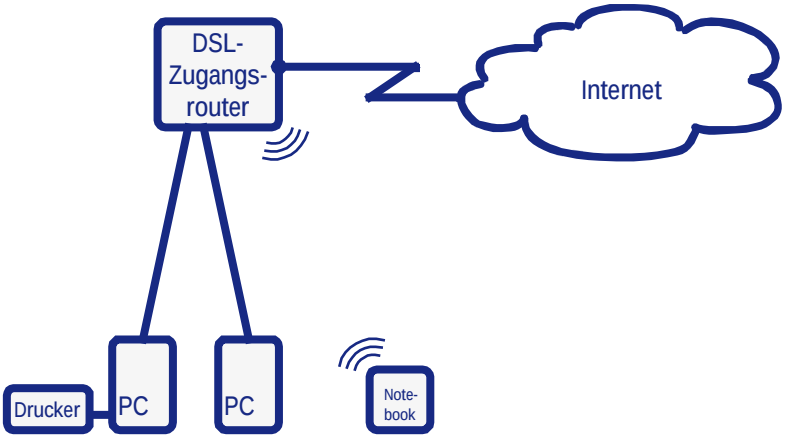
Der Zugriff auf Webseiten, die eine Authentifizierung verlangen (E-Mail, Homebanking, etc.) sollte nur über https erfolgen. Eine https-Verbindung verlangt ein Sicherheitszertifikat, das nur von einer autorisierten Stelle ausgestellt werden kann. Ist das Zertifikat dem Browser unbekannt, erhält man eine Hinweis, dass das Zertifikat ungültig, abgelaufen oder zu einer anderen Webseite gehört.

Abbildung 9: Eine https-Verbindung verlangt ein Sicherheitszertifikat, das nur von einer autorisierten Stelle ausgestellt werden kann. Ist das Zertifikat dem Browser unbekannt, erhält man eine entsprechende Meldung.

Zumindest beim Homebanking oder bei anderen vertrauenswürdigen Seiten, bei denen man anschließend einen Benutzernamen und ein Passwort eingibt, sollte man bei einer solchen Meldung misstrauisch werden und nicht automatisch eine Ausnahme hinzufügen.

Beispiele zur Internetanbindung

Die Internetanbindung zu Hause



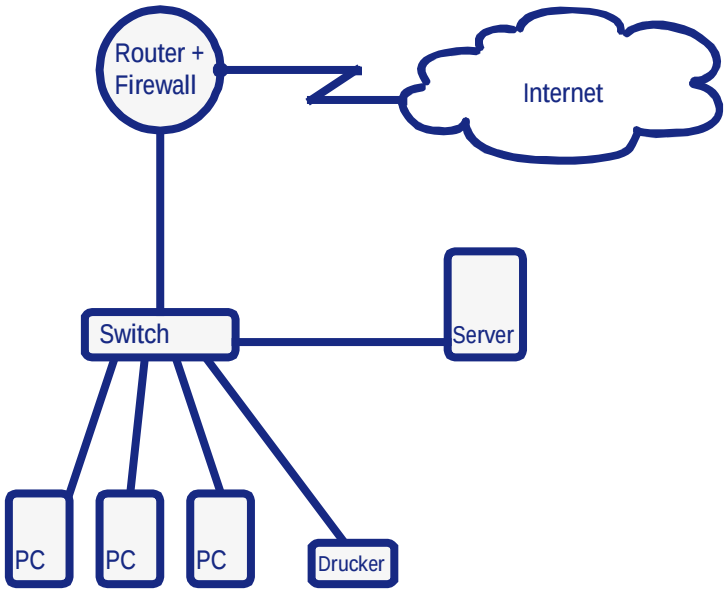
Bei einem DSL-Zugang wird am Splitter ein DSL-Router mit integriertem Modem angeschlossen. Besondere Firewall-Einstellungen am Router sind normalerweise nicht nötig, da dieser über die NAT-Funktion bereits einen guten Schutz gegen mögliche Zugriffsversuche aus dem Internet bietet. Router dieser Kategorie sind mit integriertem DSL-Modem ab ca. 50 Euro erhältlich. Einige Router ermöglichen es auch, bei der Verbindung nach außen bestimmte Dienste zu blockieren.

Die meisten Home-DSL-Router enthalten einen kleinen integrierten Switch mit 4 Ports, an den die Arbeitsplatzcomputer direkt per Kabel angeschlossen werden. Bei der Anbindung eines Notebooks über WLAN ist ein separater oder im DSL-Router eingebauter Access-Point nötig.

Soll das Funknetz nur sporadisch aktiv sein, ist es sinnvoll, wenn die WLAN-Funktion separat abschaltbar ist. Gegebenenfalls kann ein eigener Access-Point von Vorteil sein, da dieser einfach ausgeschaltet werden kann, wenn er nicht benötigt wird. Als WLAN-Sicherheitsstandard sollte WPA oder WPA2 mit einem nicht zu einfachen Passwort gewählt werden.

Der DSL-Router ist gleichzeitig ein DNS-Relay und ein DHCP-Server für das lokale Netz. Damit erhalten alle angeschlossenen Computer im lokalen Netz sofort einen Internetzugang. Der Drucker ist über USB an einem Arbeitsplatzcomputer angeschlossen und freigegeben, damit man auch vom Notebook und den anderen Computern im Netz drucken kann.

Ein kleines Unterrichts- oder Verwaltungsnetz

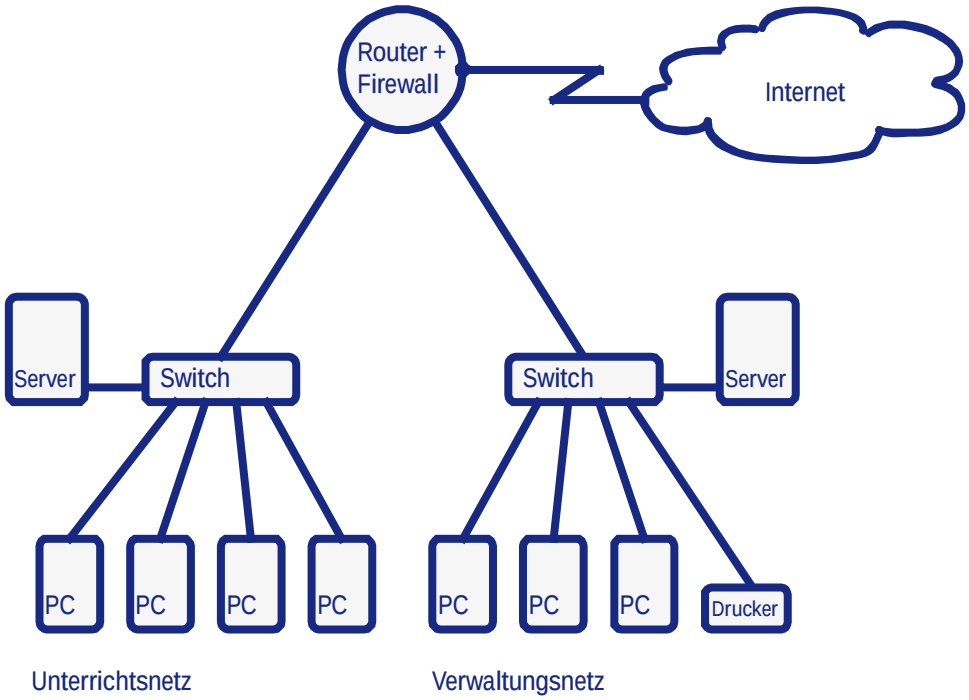


Wie bei der „Internetanbindung zu Hause“ stellt ein DSL-Router die Verbindung zum Internet her. Da normalerweise mehr Endgeräte angeschlossen werden als Switchports am Router zur Verfügung stehen und eventuell eine schnelle Serveranbindung erforderlich ist, wird ein separater Switch benötigt.

Als Router sollte ein Gerät der Preisklasse ab ca. 300 Euro gewählt werden, bei dem die Firewall exakt konfigurierbar ist. Bei einer restriktiven Konfiguration sind nur die Ports für die notwendigen Verbindungen nach außen offen (z. B. für E-Mail und Web). Der Router sollte optional auch eine Webfilterung ermöglichen (Online-Abfragen oder DNS-Filterung), um Webseiten bestimmter Kategorien zu sperren. Für diese Webfilterung können jährliche Gebühren von ca. 150 Euro anfallen.

Der Server dient zur zentralen Datenablage und stellt gegebenenfalls weitere Dienste wie DHCP oder DNS bereit, falls diese nicht vom Router übernommen werden sollen. Der Drucker ist direkt am Netzwerk angebunden, so dass jederzeit von jedem PC aus gedruckt werden kann.

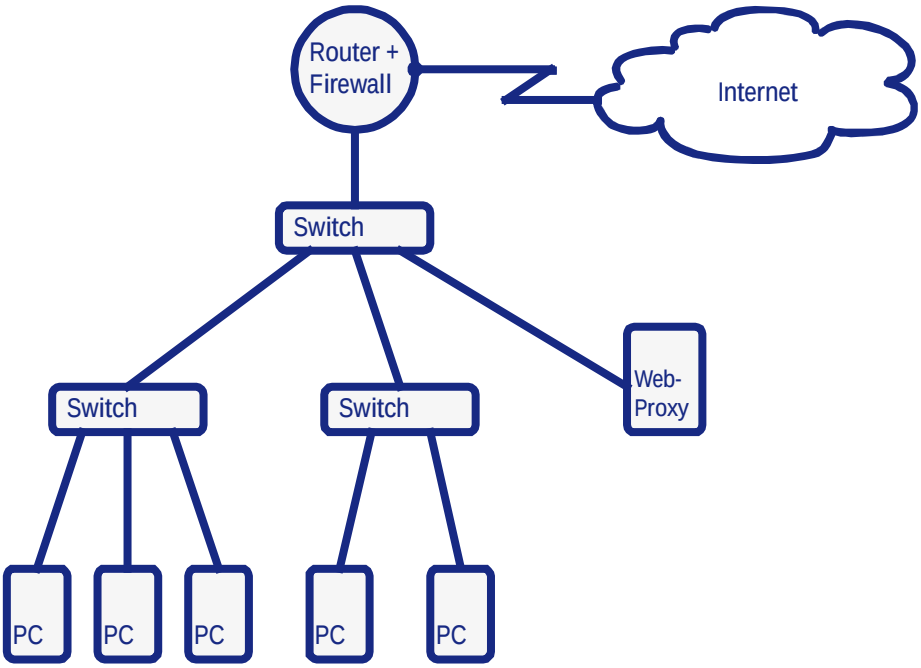
Gemeinsamer Internetzugang von Unterrichts- und Verwaltungsnetz



DSL-Router der Preisklasse ab ca. 300 Euro bieten die Möglichkeit, mehrere interne Netze mit dem Internet zu verbinden. Über die integrierte Firewall mit Zugriffskontrollisten (ACLs, Access Control Lists) lässt sich sehr differenziert regeln, wer welche Dienste nutzen kann. Im gezeichneten Beispiel ließe sich beispielsweise festlegen, dass aus dem Verwaltungsnetz auf den Server im Unterrichtsnetz zugegriffen werden kann, ein Zugriff in die umgekehrte Richtung jedoch nicht möglich ist.

Die Firewallregeln für den Internetzugang werden für beide Teilnetze getrennt geregelt. Bei einer restriktiven Konfiguration sind aus dem Unterrichtsnetz heraus nur Webverbindungen nach außen erlaubt, die zusätzlich über einen Webfilter weiter eingeschränkt werden. Aus dem Verwaltungsnetz heraus können weitere Dienste (z. B. E-Mail) ermöglicht und eventuell eine großzügigere Einstellung des Webfilters vorgenommen werden.

Internetzugang über einen Proxy-Server

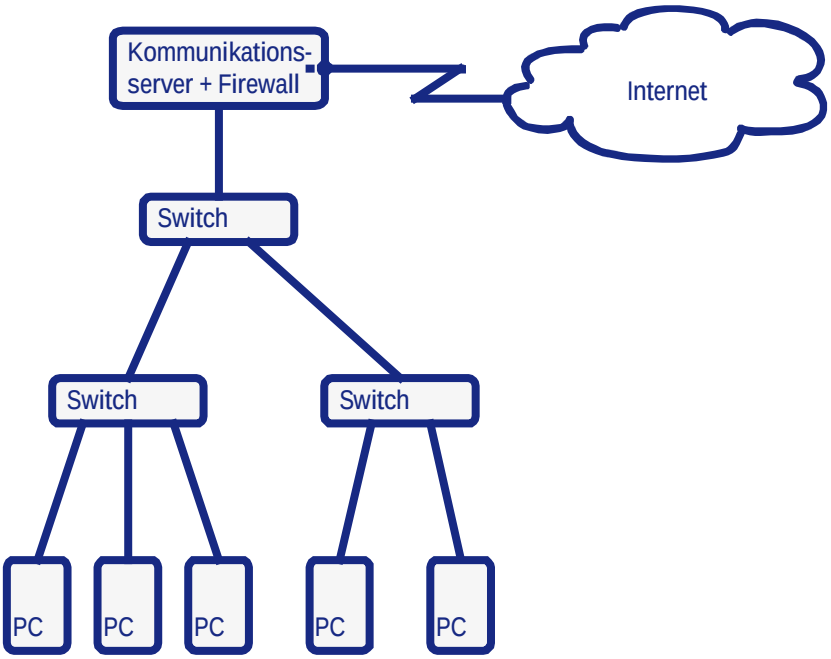


Bei einer größeren Schule mit sehr vielen gleichzeitigen Internetzugriffen kann der in einem Router integrierte Webfilter an Performance-Grenzen stoßen. Ebenso kann die Notwendigkeit bestehen, eine für die Schule individuell konfigurierbare Webfilterung mit differenzierten Einstellmöglichkeiten (z. B. zeitgesteuert oder nach Unterrichtsräumen) zu betreiben. Dazu bieten Web-Proxys derzeit eine praktikable Lösung. Die meisten zentralen Filterlösungen für das Web setzen deshalb einen Proxy-Server voraus.

Bei der dargestellten Anordnung befindet sich der Proxy im lokalen Netz, dies ist jedoch keine zwingende Voraussetzung und würde streng genommen sogar eine geringe Sicherheitslücke bedeuten. In jedem Fall müssen am Router entsprechende Filterregeln erstellt werden, damit der Zugriff auf das Web ausschließlich über den Proxy erlaubt wird. Bei einer restriktiven Konfiguration wäre nach der obigen Skizze alles gesperrt, nur der Proxy wäre in der Lage, eine Webverbindung auf Port 80 und ggf. auf Port 443 (https) aufzubauen.

Falls zusätzlich weitere Dienste (z. B. E-Mail oder FTP) ermöglicht werden sollen, müsste die Firewall gegebenenfalls dafür geöffnet werden.

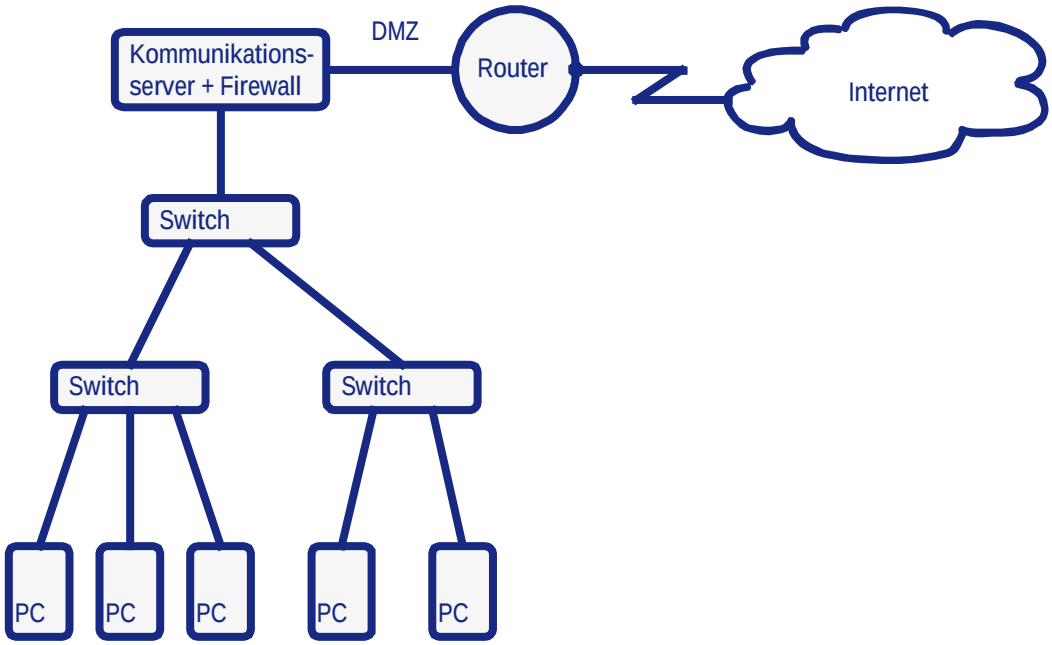
Internetzugang über einen Kommunikationsserver



Die Aufgaben eines Routers kann prinzipiell jeder Computer mit zwei oder mehr Netzwerkkarten übernehmen, auch wenn Bandbreite, Verarbeitungsgeschwindigkeit oder Sicherheit häufig nicht den dedizierten Hardwareroutern entsprechen. An Schulen ist diese Lösung dennoch beliebt, da es möglich ist, in diesen Computer neben allen Firewall-Funktionen auch einen Proxy mit Webfilterung zu integrieren.

Von verschiedenen Anbietern werden solche Kommunikationsserver (meist unter Linux) kommerziell oder als Open-Source-Lösung angeboten. Diese Systeme sind über eine Weboberfläche konfigurierbar und damit auch ohne tiefergehende Linux-Kenntnisse administrierbar. Wenn man als Kommunikationsserver keine vorkonfigurierte „Black-Box“-Lösung wählt, können die Konfiguration und die Absicherung gegen Angriffe von außen sehr komplex werden.

Internetzugang über einen Kommunikationsserver und Router



Im Prinzip ist dies eine zweistufige Sicherheitslösung, wobei der Bereich zwischen Kommunikationsserver und DSL-Router auch als DMZ (Demilitarisierte Zone) ausgebaut werden kann. Je nachdem, ob der Kommunikationsserver neben der Proxy-Funktion (mit integriertem Webfilter) auch das Routing übernimmt, hat dieser Zugang unterschiedliche Auswirkungen:

a) Kommunikationsserver ohne Routing

Wenn beim Kommunikationsserver das Routing zwischen dem internen Netz und der DMZ bewusst ausgeschaltet ist, bedeutet dies, dass aus dem internen Netz keine direkte Verbindung ins Internet möglich ist. Jede Verbindung muss über den im Kommunikationsserver integrierten Proxy laufen, der damit automatisch die gesamte Kontrolle hat. Wenn z. B. nur ein Web-Proxy installiert ist, sind andere Internetdienste nicht möglich. Da jeder Internetzugriff einen im Kommunikationsserver laufenden Proxy nutzen muss, ist dies im Prinzip die „sicherste“ aller Lösungen, die jedoch den großen Nachteil hat, dass sie sehr statisch ist und praktisch nicht erweitert werden kann.

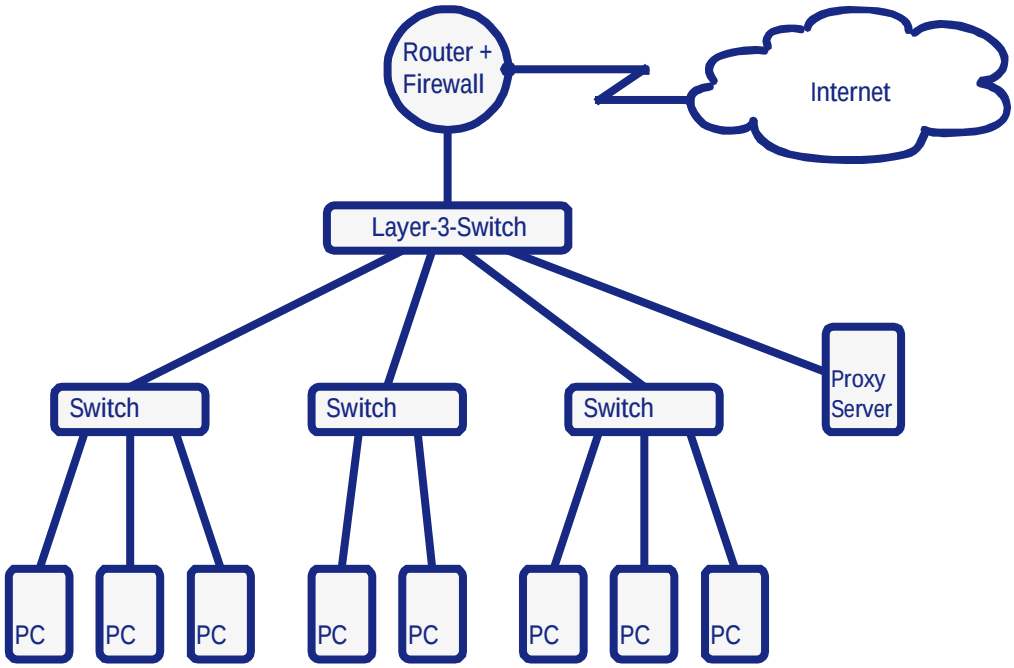
b) Kommunikationsserver mit Routing

Diese Lösung macht gegebenenfalls Sinn, wenn man eine eigene DMZ (zwischen dem Kommunikationsserver und dem Router) betreiben möchte oder den Kommunikationsserver nach außen zusätzlich absichern will. Der Kommunikationsserver übernimmt dabei wie im vorherigen Szenario alle Firewallfunktionen.

Der DSL-Router sollte mehrere interne Netze verwalten können, andernfalls müsste der Kommunikationsserver noch zusätzlich eine Netzadressübersetzung ausführen.

Erweiterungen (z. B. VPN-Zugänge von außen) sind bei einer zweistufigen Sicherheitslösung immer etwas schwieriger zu implementieren als bei einstufigen Lösungen. Gegebenenfalls muss eine zweifache Port-Weiterleitung eingerichtet werden oder der Kommunikationsserver arbeitet zugleich als VPN-Server.

Trennung eines Unterrichtsnetzes in Teilnetze

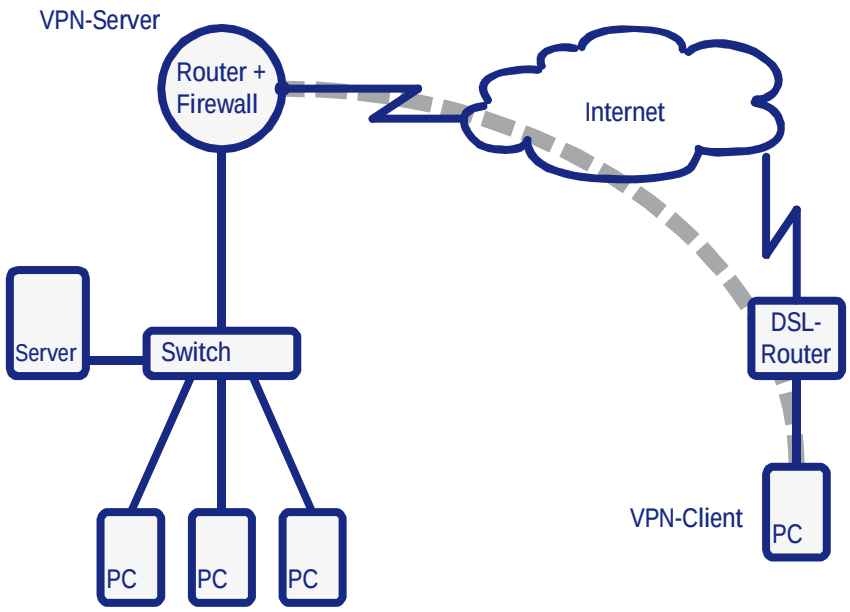


Bei vielen Computern im Unterrichtsnetz oder auch an Schulen mit getrennten Abteilungen, kann es sinnvoll sein, das Unterrichtsnetz in mehrere Teilnetze aufzugliedern. Die Trennung begrenzt die Ausbreitung von Broadcasts, reduziert damit die Netzlast und beugt auch möglichen Störungen oder Angriffsversuchen vor, da diese auf das jeweilige Teilnetz beschränkt bleiben. Der Übergang von einem Teilnetz in ein anderes Teilnetz geht über einen Layer-3-Switch, der das Routing übernimmt.

Am Layer-3-Switch wird über Zugriffssteuerungslisten (ACLs) definiert, welches Teilnetz auf welches andere Teilnetz zugreifen darf. Üblicherweise darf jedes Teilnetz auf den Server bzw. den Proxy zugreifen, der Zugriff zwischen den einzelnen Teilnetzen ist jedoch nicht erlaubt. Beim Layer-3-Switch ist auf die notwendige Bandbreite (Gigabit-Anbindung) zu achten, damit beim Serverzugriff keine Engpässe entstehen.

Die Restriktionen bezüglich des Internetzugangs werden wie bei den vorherigen Szenarien am Internetzugangsrouter eingestellt. Üblicherweise ist der Webzugriff nur über den Proxy möglich, andere Dienste sind normalerweise gesperrt, können aber auch für jedes Teilnetz separat zugelassen werden.

Zugang in das Schulnetzwerk über das Internet



DSL-Router der Preisklasse ab ca. 300 Euro bieten die Möglichkeit, über PPTP oder IPSec VPN-Verbindungen über das Internet vom Computer zu Hause in das Schulnetz aufzubauen. Vom Computer zu Hause (VPN-Client) wird nach einer erfolgreichen Authentifizierung am Schulrouter (VPN-Server) eine verschlüsselte Verbindung, die auch als Tunnel bezeichnet wird, in die Schule aufgebaut. Ein Systembetreuer, der diese Verbindung nutzt, hat damit – abgesehen von der Bandbreite – an seinem Computer zu Hause die gleichen Zugriffsmöglichkeiten, wie im internen Schulnetz.

Für den Systembetreuer oder einen Schulleiter kann diese Zugriffsmöglichkeit Vorteile bringen, wenn die Notwendigkeit besteht, von zu Hause aus in das Netz der Schule zuzugreifen. Für einen größeren Personenkreis (z. B. alle Lehrkräfte) reicht die Leistungsfähigkeit eines Routers der 300 Euro-Klasse und vor allem die Bandbreite und Zuverlässigkeit heutiger Internetanschlüsse von Schulen nicht aus.

Der Zugriff auf den DSL-Router der Schule erfolgt über dessen öffentliche IP-Adresse. Am geeignetsten ist dazu eine statische IP-Adresse vom Provider. Über verschiedene DNS-Diensteanbieter (z. B. DynDNS.com) geht es auch mit dynamischen IP-Adressen. Üblicherweise sind VPN-Verbindungen nur in Netze sinnvoll, die über eine breitbandige, nach Möglichkeit symmetrische und permanente Internetanbindung angebunden sind.

Entwicklungstendenzen bei schulischen Netzwerken

Für die Verkabelung von Schulen – zumindest bei Neu- und Umbauten – gibt es Richtlinien der Obersten Bayerischen Baubehörde, die z. B. unter http://alp.dillingen.de/service/it/richtlinien.pdf veröffentlicht sind. Diese Richtlinien sollten von Schulen unbedingt beachtet werden. Eine Nachlässigkeit in diesem Bereich führt zu Fehlern, die später ohne teure Messgeräte nur sehr schwer lokalisierbar sind und weitere Kosten verursachen.

Zunehmend kommt in Schulen auch WLAN zum Einsatz. Die zur Verfügung stehende Bandbreite ist bei den neueren Technologien meist ausreichend, falls nicht zu viele mobile Geräte gleichzeitig auf eine Funkzelle zugreifen und keine großen Datenmengen wie bei der Videobearbeitung oder dem Festplatten-Imaging transferiert werden. Eine Verkabelung der einzelnen Räume ist im Hinblick auf die Performance und die mögliche Diskussion um die Strahlenbelastung vorzuziehen (siehe auch „Votum des Beraterkreises für Schulrechner“, http://www.schule.bayern.de/votum). Da ein mit Funk abgedeckter Bereich räumlich nicht exakt begrenzt werden kann und die Zugangsdaten in der Regel innerhalb der Schule schnell bekannt sind, sollte die Nutzung auf unkritische Bereiche beschränkt bleiben und gegebenenfalls durch ein VLAN von anderen Teilnetzen getrennt sein.

Bei den aktiven Netzwerkkomponenten wie Routern, managebaren Switchen und Layer-3-Switchen war in den vergangenen Jahren ein sehr deutlicherer Preisrückgang zu beobachten. Die größeren VLAN-fähigen Switche übernehmen zunehmend mehr Routing- und Firewallfunktionen. Für schulische Netzwerke eröffnet sich dadurch die Möglichkeit, Broadcastdomänen zu verkleinern und ein lokales Netz in mehrere voneinander getrennte Teilnetze zu gliedern. Zwischen den einzelnen Teilnetzen können Sicherheitsbarrieren aufgebaut werden, so dass mögliche Störungen auf ein Teilnetz beschränkt bleiben.

Im Bereich der persönlichen Computer ist in den letzten Jahren eine Entwicklung hin zu immer mobileren und preisgünstigeren Endgeräten zu beobachten (z. B. Notebooks, Netbooks, Tablet-PCs, Smartphones oder andere WLAN-fähige Endgeräte). Die üblichen und am häufigsten an einem PC genutzten Anwendungen wie Internetbrowser, E-Mail-Client und gegebenenfalls ein Office-Paket, sind auch bei mobilen Endgeräten nutzbar.

Davon ausgehend, dass immer mehr Lehrkräfte und Schüler im Besitz solcher mobiler Endgeräte sind, eröffnet sich für Schulen die Chance, diese Geräte in das Netz einzubinden. Das Netzwerk der Schule stellt damit eine Infrastruktur mit entsprechender Verkabelung, einem abgesicherten Internetzugang, gegebenenfalls einer Funkvernetzung und einem Zugang zu einem Server in der Schule zur Verfügung. Welche Endgeräte genutzt werden, verliert – abgesehen von einzelnen branchenspezifischen Spezialanwendungen – an Bedeutung.

Gleichzeitig können „Sicherheitsaspekte“, wie Zugriffsbeschränkungen auf bestimmte Dienste und Anwendungen im lokalen Netz und im Internet, die bisher an den Arbeitsplatzcomputern ohnehin nur sehr unvollständig realisierbar waren, zu den aktiven Netzwerkkomponenten – insbesondere zum Internetzugangsrouter und zum zentralen Layer-3-Switch – verlagert werden. Der Schwerpunkt der Systembetreuung in der Schule verlagert sich damit ebenfalls von der Betreuung der einzelnen Computer hin zu den zentralen Netzwerkkomponenten.

Immer mehr Anwender verfügen über mobile Endgeräte mit eigenem Internetzugang, z. B. über UMTS oder HSDPA. Die Schule wird diese Entwicklung unter medienpädagogischen Aspekten aufgreifen müssen. Unter Sicherheitsaspekten für das Schulnetz spielt diese Entwicklung keine Rolle, da in diesem Fall nicht der Internetzugang der Schule genutzt wird.

Weiterführende Informationen

Die Systembetreuung an bayerischen Schulen wird durch die Fortbildungsinitiative SCHULNETZ unterstützt. Dazu werden allen Systembetreuerinnen und Systembetreuern in Bayern Lehrgänge zu

- „Grundlagen der Schulvernetzung“
- „Microsoft-Windows-Netzwerke“ und
- „Linux-Grundlagen“ angeboten.

Darüber hinaus finden an der Akademie für Lehrerfortbildung und Personalführung weiterführende Lehrgänge statt. Details dazu sind unter den nachfolgend genannten Links zu finden.

Ergänzend zur vorliegenden Broschüre wird der einwöchige Lehrgang „Sichere Internetanbindung von Schulen“ angeboten. In diesem Lehrgang werden die in dieser Broschüre dargestellten Konzepte von den teilnehmenden Systembetreuerinnen und Systembetreuern praktisch durchgeführt und erprobt.

Fortbildungsinitiative Schulnetz

http://alp.dillingen.de/schulnetz/

Lehrgänge an der Akademie Dillingen

http://alp.dillingen.de/lehrgaenge/suche/ (Suchbegriff: Schulnetz)

Lehrgang „Sichere Internetanbindung von Schulen“

http://alp.dillingen.de/schulnetz/internet.html