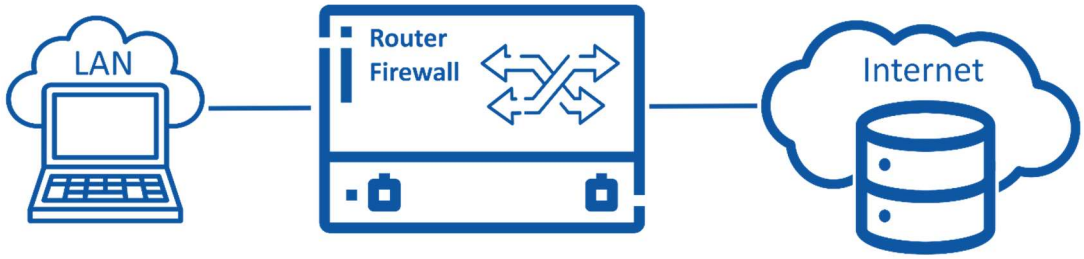
Handreichung: Router mit Firewall

Der Übergang vom sicheren Schul-LAN in das öffentliche WAN (Internet) erfolgt über den Internet-Zugangsrouter. Dieses Gerät ist von zentraler Bedeutung.

Sämtliche Internetkommunikation läuft über den zentralen Router: Er muss eine Vielzahl an Funktionen bieten, soll Sicherheit per VPN und Firewall gewährleisten, dabei stabil, zuverlässig und möglichst unauffällig über Jahre seinen Dienst verrichten. Die richtige Konfiguration ist unabdingbar, sie entscheidet über Funktionen, Performance und Datensicherheit.



Funktionsvielfalt

Routing und NAT

IP-Routing ist die zentrale Aufgabe eines Routers. Alle aktuellen Geräte unterstützen beide Versionen des Internetprotokolls, IPv4 und IPv6. Grundsätzlich sollten für die angeschlossenen Netzbereiche nur Protokolle aktiviert werden, die auch Einsatz finden.

In den allermeisten Fällen wird am Router eine Form von Adressübersetzung notwendig sein. Da im Schulnetz in aller Regel sogenannte private IPv4-Adressen zum Einsatz kommen, müssen diese in ein öffentliches Format übersetzt werden. In diesem Fall übersetzt der Router die privaten internen Adressen in eine einzige öffentliche IP-Adresse. Für diese Form der Übersetzung hat sich der Begriff NAT/NAT64 (Network Address Translation bzw. PAT) etabliert. Sämtliche Kommunikationsprozesse werden in der NAT-Tabelle des Routers geführt.

Die NAT-Funktion bietet einen positiven Nebeneffekt: Da nur ausgehende Verbindungen einen dynamischen Eintrag in die NAT-Tabelle bekommen und nur Antworten auf diese Anfragen in das LAN weitergeleitet werden, ist ein initialer Zugriff von außen nicht möglich. Ausnahmen müssen über Portweiterleitungen eingerichtet werden.

Die NAT-Adressübersetzung kann bei Routern eine leistungslimitierende Größe darstellen, wenn diese nicht für Lasten ausgelegt sind, wie sie an einer Schule vorkommen. Heimrouter, bzw. SOHO-Modelle bieten die geforderten Leistungen in aller Regel nicht. Deshalb sind sie für Schulen nicht geeignet.

Beispiel: Schule (ca. 600 SuS, LK, BYOD, WLAN)
300 SuS mit Notebook/Tablet, 600 Smartphones,
100 Schulrechner => **1000 Endgeräte**
Anz. der **Sessions** pro Endgerät ca. **20**
= 20.000 Sessions in der NAT-Tabelle

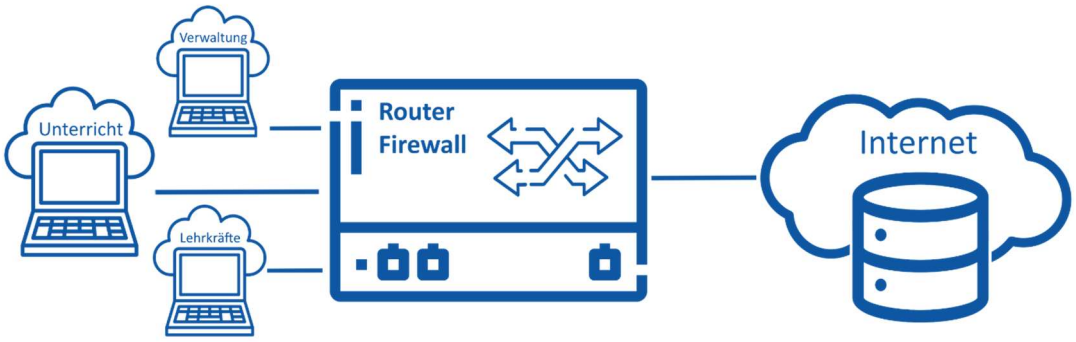
Neben der NAT-Funktion sind es die Firewall, das Routing und mögliche Zusatzfunktionen, die den Router zusätzlich beanspruchen. Ausreichende Leistungsreserven sind deshalb auch im Hinblick auf einen möglichen Glasfaserausbau an der Schule rechtzeitig zu berücksichtigen.

Wird ein Zugang aus dem Internet auf das interne Schulnetz benötigt (z.B. über VPN), ist eine feste öffentliche IP-Adresse hilfreich. Alternativ wird ein Dienst benötigt, der die öffentliche dynamische IP-Adresse zu einen festen Hostnamen auflöst (Dynamisches DNS).

LAN-Anschluss

Zur Anbindung schulinterner Netzbereiche muss der Router ausreichend viele Ethernet-Schnittstellen bieten. Kommt für das schulinterne Routing ein eigener Router bzw. Layer-3-Switch zum Einsatz, reduziert sich die Anzahl notwendiger Ports am Internetzugangsrouter. Bei manchen Modellen können LAN-Ports mittels Zuweisung von VLAN eingespart werden, indem mehrere interne Netzwerke über einen LAN-Port geführt werden können.

In kleineren Umgebungen kann der Zugangsrouter das schulinterne Routing übernehmen. Er vermittelt zwischen den Netzbereichen Verwaltung, Unterricht, Lehrernetz und dem Internet.



Firewall

Je nach Einsatzszenario überwacht und steuert die Firewall des Routers die Verbindungen zwischen LAN nach WAN, aber ggf. auch die schulinterne LAN-LAN-Kommunikation.

Eine IP-, bzw. Schnittstellen-basierte Konfiguration könnte grundlegend gestaltet werden:

von /nach >	Verwaltung	Lehrer	Unterricht	Internet
Verwaltung	-	✔	✔	✔
Lehrer	✘	-	✔	✔
Unterricht	✘	✘	-	✔
Internet	✘	✘	✘	-

✔ erlaubt ✘ verboten

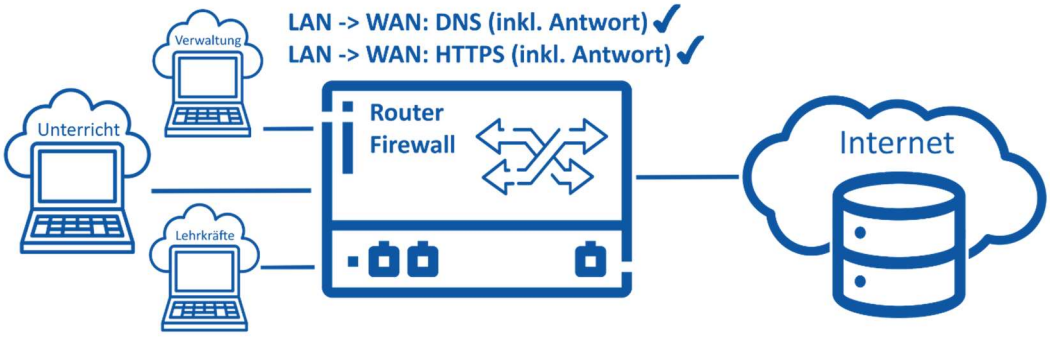
Differenzierte Firewall-Regeln ermöglichen den Zugriff, bzw. das Sperren dedizierter Protokolle und Ports. Planung, Konfiguration und Test der Firewall müssen technisch korrekt umgesetzt werden, um Sicherheitslücken auszuschließen. Die meistverwendete Umsetzungsstrategie ist sogenannte Whitelisting. In diesem Fall werden nur erlaubte Datenpakete weitergeleitet werden, alles andere ist verboten.

Die Zugriffssteuerung bzw. Access-List-Konfiguration ist von den spezifischen Gegebenheiten der Schule abhängig. Eine präzise Konfiguration und der Test aller sicherheitsrelevanten Einstellungen sind grundlegende Voraussetzungen für den Einsatz.

Alle Kommunikationsmöglichkeiten sind zu dokumentieren. Es muss sichergestellt sein, dass die erforderlichen Dienste im Schul- und Unterrichtsbetrieb funktionieren. Besonders bei interaktiven Diensten, wie z.B. Videokonferenzen ist eine Vielzahl von Ports notwendig.

Firewall-Funktionen

Das folgende Beispiel zeigt eine vereinfachte und prinzipielle Konfiguration einer (Stateful-Packet-Inspection-)Firewall. Die lokalen Gegebenheiten, das Netzdesign und die eingesetzten Geräte bestimmen letztendlich die Umsetzung.



Die unten dargestellte Zugriffsliste (ACL) enthält nur wenige Erlaubnisregeln. Alle Zugriffsregeln werden von der Firewall für jedes IP-Paket der Reihe nach abgearbeitet. Sobald eine Regel zutrifft, wird das IP-Paket entsprechend der Aktion behandelt.

In diesem Beispiel sind Anfragen aus dem lokalen Netz (LAN) auf Webserverdienste im Internet (WAN) per HTTPS (Regel 2) erlaubt. Antworten darauf werden durch diesen Firewall-Typ (SPIF) erkannt und automatisch in das LAN weitergeleitet.

Für einen Verbindungsaufbau aus dem Internet existiert in dieser Regelkette kein Eintrag, d.h., die letzte *Verbiete-Alles-Regel* wirkt und blockiert das eingehende IP-Paket. Gleiches gilt für jede Art der Kommunikation, bzw. diesen Ansatz der Konfiguration:

Alles, was nicht erlaubt ist, ist verboten!

Filterregeln				
Nr.	**Aktion**	**Quelle**	**Ziel**	**Dienst / Protokoll**
1	Erlaube	LAN	WAN*)	DNS (UDP/TCP:53)
2	Erlaube	LAN	WAN	HTTPS (TCP:443)
3	Erlaube	LAN	WAN	HTTP (TCP:80)
4	Erlaube	LAN	Router	HTTPS / SSH
(…)	(…)	(…)	(…)	(…)
n+1**)	Verbiete	ANY	ANY	ANY

LAN: Schnittstelle lokales Netz | WAN: Schnittstelle Internet | ANY: Alles

*) ggf. Adresse für spezifischen DNS-Server | **) abschließende Deny-Any-Regel (i.d.R. implizit)

Zugang und administrativer Zugriff

Ausschließlich autorisiertes Personal darf Einstellungen und Änderungen am Internetzugangsrouter vornehmen. An zentraler Stelle, z.B. Schulleitung oder Schulaufwandsträger, muss festgehalten werden, wer physisch und administrativ Zugriff auf das Gerät hat. Im Schulbetrieb könnten dies Mitarbeiter des Schulaufwandsträgers, die von der Schulleitung beauftragte Systembetreuung oder ein beauftragter Dienstleister sein.

Zentrale Geräte der Schul-IT sind an einem nicht allgemein zugänglichen Ort, meist der Serverraum bzw. verschlossene Netzwerkschränke, zu betreiben. Nur autorisiertes Personal hat den physischen Zugriff auf die sensiblen Systeme der Schulnetzinfrastruktur.

Checkliste: Physischer Zugang zur IT-Infrastruktur

	Serverraum	NW-Schrank-LAN	NW-Schrank-WAN	Stockwerks-verteiler
Hausmeister	✔	✘	✘	✘
Schulleitung	✔	✔	✔	✔
Systembetreuer	✔	✔	✔	✔
Ext. Techniker	○	✘	✘	✘

○ in Begleitung, bzw. in Servicefällen

Administration

Die zentralen IT-Systeme sind in besonderer Weise zu schützen. Der administrative Zugriff ist deshalb auf den unbedingt notwendigen Personenkreis einzuschränken. Zentrale Geräte, wie zum Beispiel der Firewall-Router, bieten mitunter den Zugriff auf alle übertragene Nutzdaten. Sie sind aus Sicht des Datenschutzes als sensibel zu betrachten. Falls notwendig und sinnvoll, kann, je nach Gerät bzw. Hersteller, zwischen nur lesendem und einem Vollzugriff auf den Router unterschieden werden (Rollenkonzept). Der administrative Zugriff über Protokolle (SSH, Telnet, HTTP/S) und Schnittstellen (LAN, Konsole etc.) muss reglementiert sein.

Zugang NW-Geräte:

	Router Internetzugang	Layer-3-Switch LAN	WLAN-Controller	L2-Switch
Schulleitung	(✔)	(✔)	(✔)	(✔)
Systembetreuer	✔	✔	✔	✔
Ext. Techniker	○	○	○	○

(✔) Zugangskennung unter Verschluss ○ temp. Zugang, bzw. in Servicefällen

Zugang Firewall-Router:

	Konsole	SSH	HTTP/S	VPN/IPsec	Telnet
Schulleitung	(✔)	(✔)	(✔)	(✔)	✘
Systembetreuer	✔	✔ nur intern (LAN)	✔ nur intern (LAN)	✔	✘
Ext. Techniker	○	○	○	○	✘

(✔) Zugangskennung unter Verschluss ○ temp. Zugang, bzw. in Servicefällen

Anforderungen Firewall

Die Firewall-Funktion ist in aller Regel Teil des Routers. Dedizierte Firewall-Systemen sind für den Einsatz an Schulen im Funktionsumfang oft überdimensioniert. Die Leistungsfähigkeit des Gerätes muss alle Funktionen in der gebotenen Bandbreite abdecken.

Anforderungen:

- Anbindung von mehreren IP-Netzen nach Bedarf (insb. LAN).
- Differenzierte Regelerstellung auf Basis von IP-Adressen, Schnittstellen, Protokollen und Ports für ein- und ausgehenden Datenverkehr.
- Firewalltyp SPIF (Stateful-Packet-Inspection-Firewall), prüft dynamisch ein- und ausgehende Pakete. Die eher geringen Anforderungen an die Hardware ermöglichen den Einsatz auf Internetzugangsroutern.
- Inhaltsbasierte Filterung erfordert den Einsatz eines Proxies (Application-Level-Gateway). Dieses Konzept ist für den allgemeinen Unterrichtsbetrieb unter Einsatz mobiler Endgeräte in aller Regel schwierig und wird nicht empfohlen. Die aufwändige Filterung setzt den Einsatz leistungsfähiger Hardware voraus (Appliance bzw. dedizierte Rechner).
- Eine grafische Benutzeroberfläche erleichtert oft die Konfiguration und Funktionsübersicht, ist aber nicht funktionsrelevant.
- Nach abgeschlossener Konfiguration sollte die gewünschte Funktion bzw. Nicht-Funktion geprüft werden. Ein Portscan zeigt die Sperr- bzw. Weiterleitungsfunktion der Firewall.
- Firmware-Updates müssen vom Hersteller bereitgestellt und einfach installierbar sein.
- Konfigurationsdateien können verschlüsselt exportiert werden.

Support, Ersatz, Redundanz

Der Internetzugangsrouter spielt eine zentrale Rolle in der unterrichtlichen und organisatorischen Arbeit an der Schule. Geräte bzw. Hersteller aus dem Business-Umfeld bieten die geforderten Eigenschaften.

Ein Ausfall des Routers muss unverzüglich kompensiert werden. Denkbar sind in diesem Zusammenhang Supportverträge, die einen kurzfristigen Hardware-Austausch ermöglichen. Schon bei der Beschaffung ist auf diesen Aspekt der Verfügbarkeit zu achten. Alternativ ist es möglich, ein typgleiches Ersatzgerät bereitzuhalten. Der kurzfristige Einsatz eines Ersatzgerätes setzt voraus, dass eine aktuelle Konfigurationsdatei des Produktivsystems vorhanden ist. Diese muss an einem sicheren Speicherort in der aktuellen Version vorgehalten werden.

Der Ausfall einer Internetverbindung kann durch redundante Anbindungen kompensiert werden. Neben einer Festnetzzugangstechnik könnte eine Mobilfunkverbindung (LTE/5G) einspringen und die Grundversorgung aufrechterhalten.