



## Absicherung des Internetzugangs

Dienste und Daten eines Netzwerkes mit Internetanschluss sind ohne geeignete Schutzmaßnahmen für jeden Internetanwender nutz- und einsehbar. Selbst Einzelrechner sollten heutzutage nicht mehr direkt ans Internet angeschlossen werden oder allenfalls nach Abschaltung sämtlicher nicht benötigter Netzwerkdienste. Als Schutzmaßnahme können der Internet-Leitung sog. **Firewalls** vorgeschaltet werden.

Es gibt verschiedene Arten von Firewalls, die sich durch unterschiedliche Schutzmechanismen und Sicherheitslevel voneinander unterscheiden. Gemeinhin handelt es sich bei einer Firewall um eine externe unabhängige Komponente, sei es eine spezielle Software auf einem dedizierten Server, sei es ein Hardware-Router mit Firewall-Funktionalität. Wenn ein Firewall-Programm auf dem zu schützenden Rechner direkt installiert wird, spricht man von einer **Personal Firewall**. Diese sollte lediglich verwendet werden, wenn ein nicht vernetzter Einzelrechner sich direkt mit dem Internet verbinden soll (z.B. Laptop auf Geschäftsreise), da ansonsten bei übrigem Netzwerkbetrieb Probleme mit dem Zugriff auf externe Ressourcen (z.B. Laufwerksfreigaben) entstehen könnten. Für den stationären Betrieb empfiehlt sich aber auch dann eine externe Firewall, wenn lediglich ein Rechner mit dem Internet verbunden werden soll, da unbedachte Benutzerhandlungen, Programm-Sicherheitslücken oder gar auf den Rechner gelangte Trojaner die Personal Firewall stören oder gar ganz abschalten könnten.

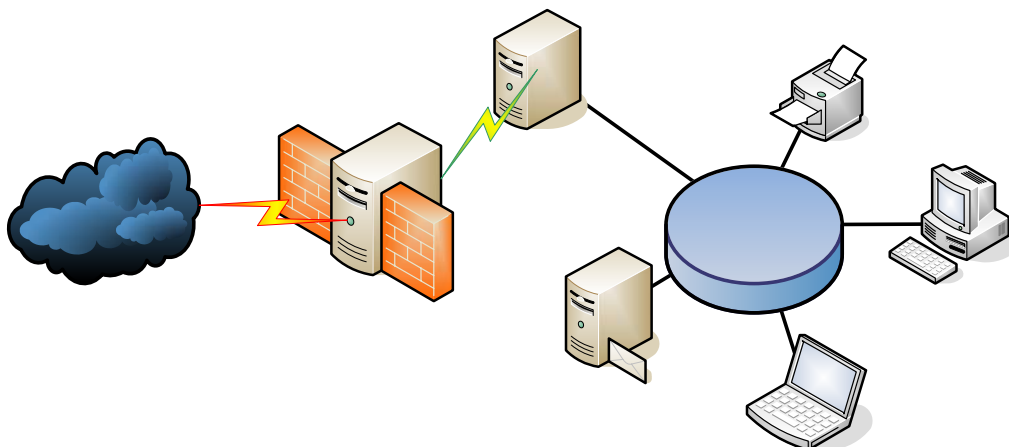
Folgende Firewall-Schutzmethoden stehen zur Verfügung, wobei diese durchaus auch kombiniert eingesetzt werden:

**Paketfilter** (Screening Router) filtern den Datenstrom lediglich auf der Paketebene anhand von Quell- und Zielports sowie Quell- und Zieladressen. Sie dienen dazu, Kommunikationsdienste und den Zugriff auf Systeme zu beschränken. Diese Funktion wird oft von einem Router übernommen. Es finden keine inhaltlichen (z.B. Viren) oder

nutzerbezogenen Überprüfungen statt. Daher stellen reine Paketfilter eine eher schwache Variante einer Firewall mit niedrigem Sicherheitsstandard dar.

Eine **Stateful Inspection Firewall**, auch bekannt als dynamischer Paketfilter, ist in der Lage, aktuelle Merkmale einer Kommunikationsverbindung zu erkennen und diese bei der Filterung des Datenstroms zu berücksichtigen. Auf diese Weise lassen sich beispielsweise manipulierte Verbindungen erkennen. Stateful Inspection Firewalls bieten einen größeren Leistungsumfang als Paketfilter und daher auch eine höhere Schutzfunktion.

Ein **Application Level Gateway**, auch Proxy-Firewall genannt, analysiert den Datenstrom auf Anwendungsebene, wodurch inhaltliche Bewertungen von Daten, wie z.B. Benutzerauthentifizierungen und Virenüberprüfungen, erst möglich werden. Bei einem Application Level Gateway werden nicht einzelne Ports offen gelassen, sondern der Datenverkehr wird über Proxies abgewickelt, die Anfragen für jeweilige Dienste entgegennehmen und bearbeiten und somit keine direkten Kommunikationsverbindungen zwischen Quelle und Ziel zulässt.



Einfache Firewalls wie sie beispielsweise in DSL-Routern eingesetzt werden, verfügen meist nur über Paketfilter, Firewall-Software zum Einsatz auf Serverhardware sollte alle drei Methoden beherrschen.

Welche Firewall-Lösung in einem spezifischen Fall verwendet werden sollte, hängt sowohl von der Art der Internet-Anbindung ab als auch von den Diensten im internen Netzwerk, auf die vom Internet aus zugegriffen werden soll. Eine Auswahl sollte daher in Zusammenarbeit mit erfahrenen IT-Beratern stattfinden.