* + 1. **Firewall**

**Theoretische Grundlagen**

Die grundlegende Aufgabe einer Firewall ist der Schutz des Rechners von außen. Einfach erklärt werden in der Firewall bestimmte Regeln und Filter im Vorhinein definiert und angewandt. So können schädliche Daten frühzeitig entdeckt und abgeblockt werden. Durch den Gebrauch von Firewalls werden Firmen oder auch Privatnutzer vor Viren geschützt. Dadurch kommt es auch zu keinem Datenverlust. Ebenfalls schützt die Firewall vor unbefugten Zugang auf sensible Daten.

In der IT-Geschichte haben sich bis heute fünf wesentliche Firewall-Typen herauskristallisiert, welche in den folgenden Kapiteln genauer beschrieben werden.

**Paket Filter**

Die Software für diesen Filter findet Anwendung bei wichtigen Punkten im System, wie dem Router oder dem Switch. Der Paket-Filter prüft dauerhaft den Datenverkehr der Pakete, die eingehen und ausgehen. Die Kontrolle basiert auf zuvor festgelegten Sicherheitsrichtlinien. Dazu gehören Kriterien wie die Portnummer, IP-Adresse oder Pakettype. Dazu werden Richtung, Ziel- und Quelladresse analysiert. Falls das Gerät Pakete erkennt, die nicht den gewollten Regeln entsprechen, werden sie nicht ins interne Netz weitergeleitet.

Zu erwähnen ist jedoch noch, dass diese Art der Firewall nicht die Sicherste ist. Zum einen können bei der Einrichtung der Sicherheitsregeln viele Fehler passieren und zum anderen schützt er nicht vor Absenderfälschungen, daher wird diese als die schwächste der möglichen Firewall Varianten bezeichnet.

**Circuit Level Gateway**

Die TCP-Dateien im gesamten System werden überwacht. Dadurch ist eine relativ schnelle Identifikation bösartiger Dateien möglich. Es wird festgestellt, ob die geöffnete Sitzung sicher ist. Es wird zwar ermöglicht, dass spezifische Ports oder IP-Adressen gezielt gesperrt werden können, aber die Bestimmung des Paketinhaltes ist nicht möglich.

**Stateful Inspection Firewall**

Stateful Inspection Firewalls analysieren jedes Paket und untersuchen gleichzeitig, ob dieses Paket Teil einer autorisierten TCP-Sitzung ist. In jeder Session werden Port, Quell-/ und Zieladresse überwacht. Nicht autorisierte Pakete werden sofort abgewiesen. Diese Variante ist zwar sicherer, ist aber auch mit einer höheren Belastung der Netzwerkleistung verbunden.

**Proxy-Firewall**

Dieser Sicherheitsmechanismus arbeitet auf dem Application-Layer. Er überwacht, anders als der Paket-Filter, nicht nur spezifisch programmierten Pakets, sondern analysiert den Traffic auf dem Application-Layer. Die Proxy-Firewall agiert zwischen eigenem und fremdem Netzwerk. Anfragen aus dem Internet werden abgefangen, gefiltert und analysiert und anschließend stellvertretend weitergeleitet oder eben abgeblockt. Jedes Protokoll, wie HTTPS, SMTP oder DNS bekommt einen eigenen Filter, der bestimmte Datenkommunikation verbieten und herausfiltern kann. Diese Art der Firewall ist sehr sicher, da das eigene und das fremde Netzwerk quasi nie miteinander direkt verbunden ist.

**Next-Generation Firewall**

Die Next-Generation Firewall, kurz NGFW, beschreibt die dritte Generation der Firewall-Technologie. Um gegen moderne Viren und Bedrohungen zu schützen sind Firewalls, die bestimmte Ports filtern, oft nicht mehr ausreichend. Das ist darauf zurückzuführen, dass Viren oft über Port 80, bzw. Port 443 in das private Netz eindringen. Die Next-Generation Firewall untersucht nicht nur Protokoll und Port, sondern erkennt ungewöhnlichen Datenfluss und filtert abnormale Dateien weg. Next-Generation Firewalls besitzen unter anderem auch Antiviren-, Anti-Spam Filter und ähnliche Funktionen. Durch die zusätzlichen Features werden Extra-Security Gateways, Proxys oder ähnliche Softwaresysteme überflüssig.

.

* + 1. **Firewall**

Moderne Linux Kernel werden standardmäßig mit dem so genannten Paket-Filtering ausgestattet. Dieser entscheidet, welcher Traffic an den Server weitergeleitet wird, und welcher abgeblockt wird.

Das Standard Firewall System für Ubuntu ist ufw (Uncomplicated Firewall). Diese Firewall wird mit “sudo ufw enable” eingeschalten, bzw. mit “sudo ufw disable” ausgeschalten. Port 22 (SSH) wird mit “sudo ufw allow 22” konfiguriert. Um die Liste dieser erlaubten Ports zu nummerieren, kann der Befehl auch als “sudo ufw insert 1 allow 80” (am Beispiel Port 80) geschrieben werden.

Gleich wie eine Regel hinzugefügt wird, könnte sie durch den Befehl “sudo ufw deny 22” geschlossen, oder mit “sudo ufw delete deny 22” gelöscht werden. Das wurde für die in der Diplomarbeit angeführten VM nicht gemacht.

Der Befehl “sudo ufw –dry-run allow http” ermöglicht es die Auswirkung des Kommandos “sudo ufw allow http” trocken (also theoretisch) durchzuspielen.

In weiterer Folge werden drei verschiedene Varianten in Form von Abbildungen dargestellt, den Firewall Status anzeigen zu lassen.

1. sudo ufw status:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

**Abbildung 32 Firewall; sudo ufw status**

* Es werden die wichtigsten Daten zum Status der Firewall angezeigt.

1. sudo ufw status verbose:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

**Abbildung 33 Firewall; sudo ufw status**

* Detaillierte Auflistung der Firewall-Daten.

1. sudo ufw status numbered:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

**Abbildung 34 Firewall; sudo ufw status numbered**

🡪Zeigt die Liste gleich wie Punkt a) an, mit dem Unterschied, dass die Tabelle nummeriert, angezeigt wird