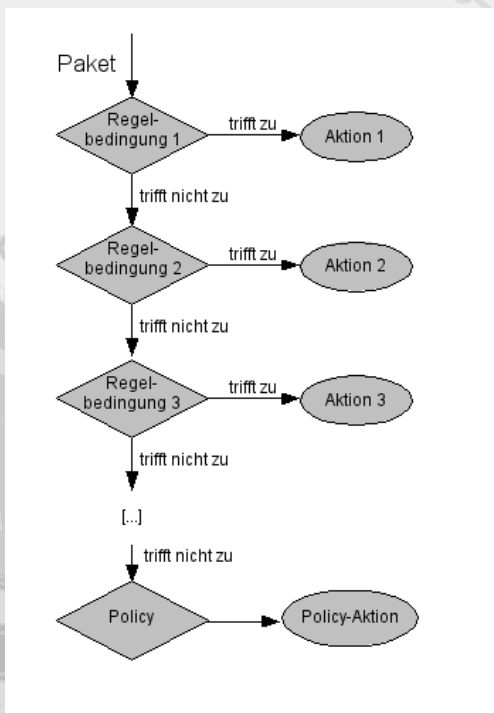


DECO_Firewall

Das Internet bietet sehr viele Möglichkeiten um effizient zu kommunizieren und Daten auszutauschen. Allerdings hat sich das Internet auch zu einer Spielwiese für Hacker entwickelt. Das man sich davor schützen muss, ist inzwischen jedem bewusst geworden. Allerdings stellt sich die Frage wie man dies am besten macht, ohne seine eigenen Arbeitsprozesse zu beschneiden und welche Kosten für ein Firewall-System auf das Unternehmen zukommen. Hinzu kommt, dass es sehr unterschiedliche Firewall-Typen auf dem Markt gibt (Paketfilter, Application Level Gateway, Screened Gateway), die unterschiedliche Vor- und Nachteile sowie Preisgestaltungen besitzen.

Eine Entscheidungsgrundlage welche Firewall für ihr Unternehmen die richtige ist bietet die Analyse der individuellen Kommunikationsprozesse von und zum Internet, die es abzusichern gilt. Die Firewall übernimmt dabei die Aufgabe eines Gateways, die ein Werkzeug für die Abbildung des Sicherheitskonzepts darstellt. Die Kommunikationsabläufe zwischen den Übergangspunkten werden an zentraler Stelle von der Firewall kontrolliert.



Neben professionellen Lösungen von Checkpoint und CyberGuard bietet die DECOIT GmbH auch preiswerte Open-Source-Alternativen an. Auf Basis des Linux-Kernels (ab 2.4) kann eine Paket- und Port-basierte Firewall über iptables aufgebaut werden, die eine hohe Performance besitzt. Der interne Filter wird über ein Regelwerk angesprochen, welches aus der Security Policy des Unternehmens abgeleitet wurde. Das Programm ip-

tables kommuniziert mit dem Linux-Kernel und weist diesen an, Pakete nach bestimmten Regeln zu filtern (siehe Abbildung). Iptables übernimmt also unter anderem das Einfügen, Löschen und Manipulieren von Regeln in die Filtertabellen des Kernels sowie das Setzen der Filterpolitik. Dabei ist auch das Clustern solcher Systeme ohne Probleme möglich, um die Verfügbarkeit auf ein Höchstmaß zu bringen.

Die DECO_Firewall besitzt folgende Hauptmerkmale:

1. Regelbasierte Paket-Firewall, die ohne Lizenzkosten auskommt
2. Lauffähig auf einem herkömmlichen Serversystem
3. Leistungsstarkes System mit hoher Performance
4. Die Anpassungen des Regelwerks ist auch grafisch möglich (einfachere Handhabung)
5. Durch die Clustermöglichkeit besteht eine sehr hohe Verfügbarkeit von nahezu 100%
6. Ausführliche Mitschreib-Möglichkeiten der erlaubten und nicht erlaubten Zugriffe
7. Automatische Benachrichtigung durch E-Mail bei Ausfall des Clusters

Die iptables selber werden vom Netfilter-Projekt-Team gepflegt und kontinuierlich weiter entwickelt, welches durch eine kleine Gruppe von Entwicklern 1999 ins Leben gerufen wurde. Iptables ist seit 2000 unter der GNU General Public License (GPL) verfügbar. Die DECO_Firewall fügt diverse Filter in den Kernel ein, löscht andere und verwaltet bestehende Filterregeln. Zusatzfunktionen können per Kernel-Modul ein- und ausgeschaltet werden. Die DECO_Firewall ist außerdem in der Lage verbindungsorientierte Protokolle wie File Transfer Protocol (FTP) zu handhaben. Eine Unterstützung für Network Address Translation (NAT) ist ebenfalls vorhanden.

Als Hardwareausstattung reicht ein konventioneller Server, der allerdings professionellen Ansprüchen genügen sollte. Generierte Logfiles können bei ausreichender Festplattenkapazität auf der Firewall selbst mitgeschrieben werden.

Komponenten:

- Linux-Betriebssystem ab Linux Kernel 2.4
- Regelwerk auf iptables-Basis
- Webmin-Oberfläche zur Regel-Konfiguration

Systemanforderungen:

- Linux-Betriebssystem
- 2 GHz CPU mit 512 MByte RAM
- 120 GByte SATA Festplatte