6.3. Was ist eine DMZ

Die demilitarisierte Zone, kurz DMZ, ist ein Netzwerk, welches sich logisch gesehen zwischen zwei Firewalls befindet. Falls dieses Konstrukt mit effektiv zwei Firwalls realisiert wird, sprechen wird von einem zweistufigen Firewall-Konzept.

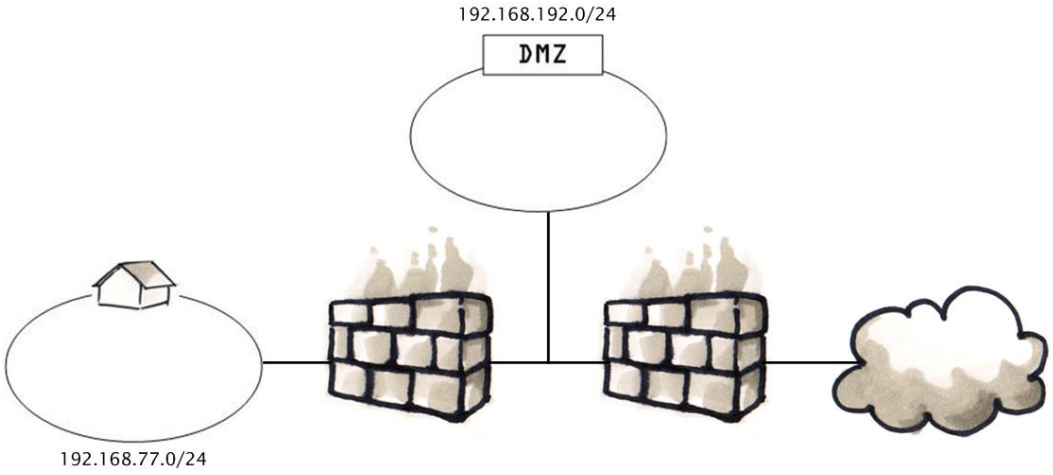

Abbildung 6.3.: Zweistufiges Firewall-Konzept mit DMZ

Im Bereich der kleinen und mittleren Unternehmen treffen wir jedoch meist nur eine logische Form des zweistufigen Konzeptes an oder anders gesagt, wird die Form der zweistufigen Konzeption innerhalb der Firewall realisiert. Dies geschieht durch ein erweitertes Regelwerk sowie durch eine physikalisch vorhandene weitere Netzwerkschnittstelle, die den Betrieb einer DMZ ermöglicht. Das heisst, in unserem Fall besitzt die Firewall 3 Interfaces.

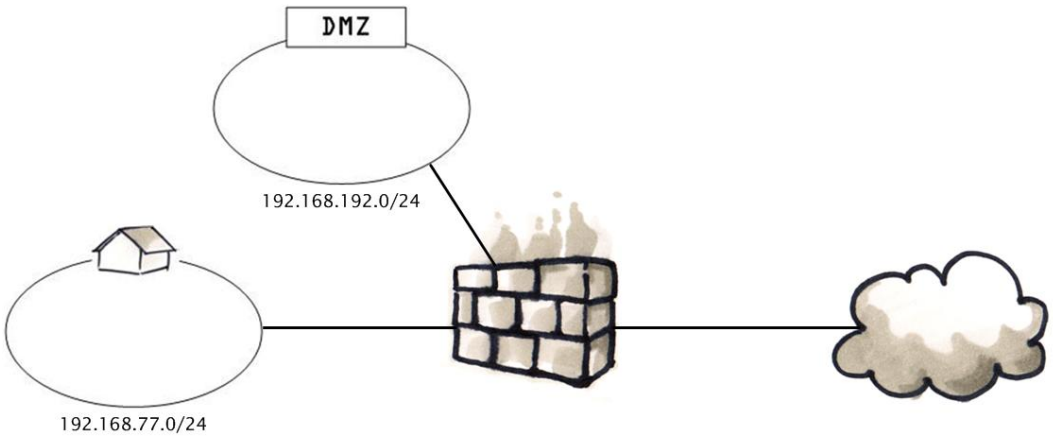

Abbildung 6.4.: Firewall mit dediziertem DMZ-Port

Doch wo genau kommt nun eine demilitarisierte Zone zum Einsatz und was sollte in ihr betrieben werden und was besser nicht? Diese Frage lässt sich leider, ohne Kenntnisse der Umgebung, nicht zu 100% beantworten. Was aber sicher ist, ist, dass eine DMZ, oder auch *Screened Subnets* genannt, eine Plattform für den Betrieb von exponierten Servern darstellt.

Grundlegend kann gesagt werden, dass eine DMZ ein eigenständiges Netzwerk ist inkl. eigenem IP-Adress-Konzept, Subnetzmaske und einem eigenen Gateway. Verwaltet wird das DMZ-Netz jedoch aus dem produktiven LAN oder über eine dedizierte Administrationskonsole - dies hängt von Ihren Möglichkeiten und Geldern ab. Sinn und Zweck einer DMZ wäre jedoch, so wenig Brücken ins produktive LAN zu schlagen wie nur möglich.

Das heisst nun für Sie, dass Server, welche direkt vom externen Netz angesprochen werden können, beispielweise ein Webserver, FTP-Server oder eMail-Server, nicht in das produktive LAN gehören und somit ihren Platz in der demilitarisierten Zone finden.

Stellen Sie sich vor, was geschehen würde, wenn ein Angreifer erfolgreich Ihren Webserver in seinen Besitz nehmen könnte. Er hätte dann, je nach Kenntnissen und Möglichkeiten des Übeltäters, Zugriff auf sämtliche Ressourcen innerhalb Ihrer produktiven Umgebung.

Um dieses drohende Risiko abzuschwächen, platzieren Sie diese Server am besten in der DMZ. Falls nun ein erfolgreicher Angriff durchgeführt wird, kann sich der Hacker/Cracker höchstens innerhalb der DMZ verwirklichen, die Hürde ins LAN ist somit noch nicht genommen.

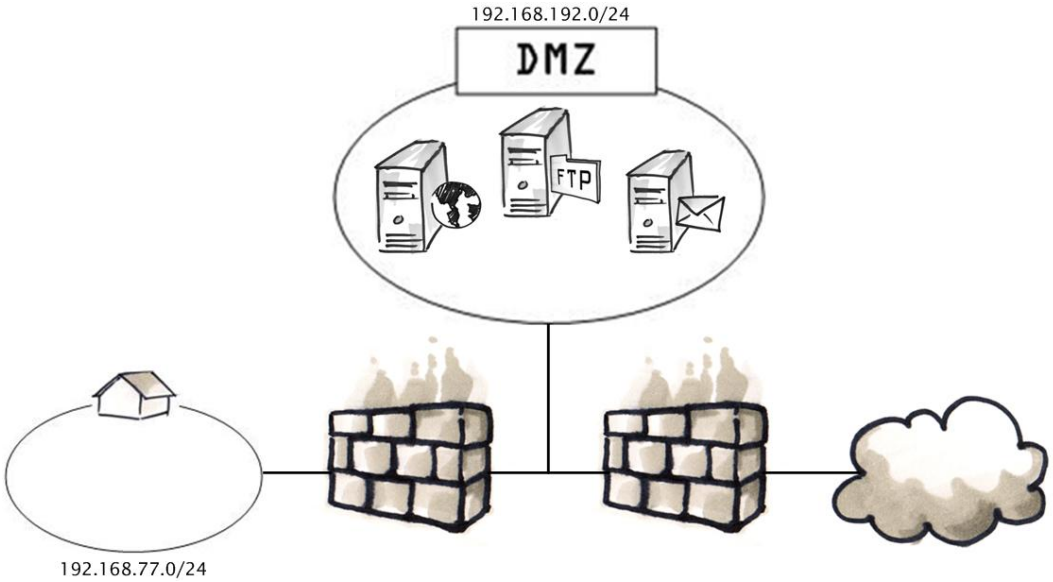

Abbildung 6.5.: Firewall mit dediziertem DMZ-Port