Doppelte Portweiterleitung oder: Wie kann man Rechner hinter einer Routerkaskade erreichen?

In meinem Beitrag Einrichten einer echten DMZ mit zwei Fritz!Boxen habe ich aufgezeigt, wie man mit 2 Fritz!Boxen zu einer echten Hardware-DMZ kommen kann, um sein privates Netz in eine dem privaten Netz vorgelagerte „rote“ Zone und eine abgesicherte nachgelagerte private „blaue“ Zone unterteilen kann.

Immer wieder erreichen mich Nachfragen, ob es denn nicht trotzdem möglich sei Rechner-IPs aus dem privaten „blauen“ Netz von seiten des Internets zu erreichen?

Zu der Thematik hat auch Ernst Ahlers von der c’t aus dem heise Verlag einen schönen Artikel verfasst, den man unter Router Kaskaden aufrufen kann.

Ganz abgesehen davon, dass man sich dazu Gedanken machen sollte, ob so etwas überhaupt sinnvoll ist, so kann es doch Szenarien geben, die dies sinnvoll erscheinen lassen: z.B. eine VPN-Verbindung in das blaue Netz. Oder ein Server steht aus gutem Grund im blauen Netz und soll doch von außen erreichbar sein.

Die Lösung ist eigentlich recht einfach und Ihnen sicherlich schon in Teilen bekannt: man löst dies mit einer doppelten Portweiterleitung.

Machen wir ein einfaches Beispiel und treffen ein paar Annahmen:

- Sie haben ihr Netz in einen „roten“ Aussenbereich und

einen „blauen“ geschützten Bereich segmentiert. Es spielt dabei keine Rolle, ob sie das per Hardware-DMZ oder anderweitig gelöst haben.

- Ihr rotes Netzwerk, dass direkt mit dem Internet verbunden ist, hat in unserem Beispiel folgende Daten:
  - Router „rot“ hat die interne IP-Adresse: 192.168.0.1
  - Router „rot“ hat auch eine externe IP-Adresse, die im Normalfall durch den Provider zugeordnet wird. Mit dieser IP ist häufig auch gerade bei DSL-Anschlüßen mit wechselnden IPs die vom Provider zugeteilt werden, eine dynamischer DNS-Dienst verbunden (z.B. selfhost.eu oder dyndns.org, etc.). In unserem Beispiel wäre dies „beispiel.selfhost.eu“
- Ihr blaues geschütztes Netzwerk hat die folgenden Daten
  - Router „blau“ hat die externe IP-Adresse 192.168.0.254
  - Das durch den Router „blau“ verwaltete interne Netz lautet z.B. 192.168.178.XXX
- Sie wollen jetzt auf den Rechner 192.168.178.99 auf dem in unserem Beispiel ein Webserver auf Port 80 läuft von außen zugreifen. Das ist mal der Plan – schauen wir wie wir das umsetzen…

Die Lösung: doppelte Portweiterleitung:

1. Sie richten eine Portweiterleitung auf dem roten Router ein und zwar von Port 80 auf Port 80 mit dem Ziel 192.168.0.254 (also der externen IP unseres blauen Routers). Alle Pakete die auf dem roten Router auf Port 80 extern aus dem Internet ankommen werden mit dieser Weiterleitung an den blauen Router auf Port 80 weitergereicht.
2. Sie richten eine weitere Portweiterleitung auf dem blauen Router ein. Und zwar von Port 80 auf Port 80 mit dem Ziel 192.168.178.99. Damit werden alle Pakete von

Port 80 an den Zielrechner auf Port 80 weitergeleitet.

Sie können jetzt von extern mit der Adresse „http://beispiel.selfhost.eu:80“ auf den im blauen Netz stehenden Webserver zugreifen.

Fertig.