## 3.3 Praktische Aufgaben

In diesem Praxis-Teil werden die Dienste FTP (siehe Seite 164), Telnet (TCP Port 23), SSH (TCP Port 22), DNS (nur Abfragen, UDP Port 53, siehe Seite 145) und NTP (UDP Port 123, siehe `man ntp`), SMTP (TCP Port 25) und der TCP-Proxy-Port 3128 durch Paketfilterregeln abgesichert.
Auf dem `secserver` ist ein DNS-Dienst aktiv, tragen Sie diesen in Ihrem Rechner als DNS-Server ein. Ebenso läuft auf dem `secserver` der NTP-Dienst.
Alle für unsere Versuche benötigten Netfilter-Pakete sind schon auf den Rechnern installiert.

### 3.3.1 Umstellung der Netztopologie

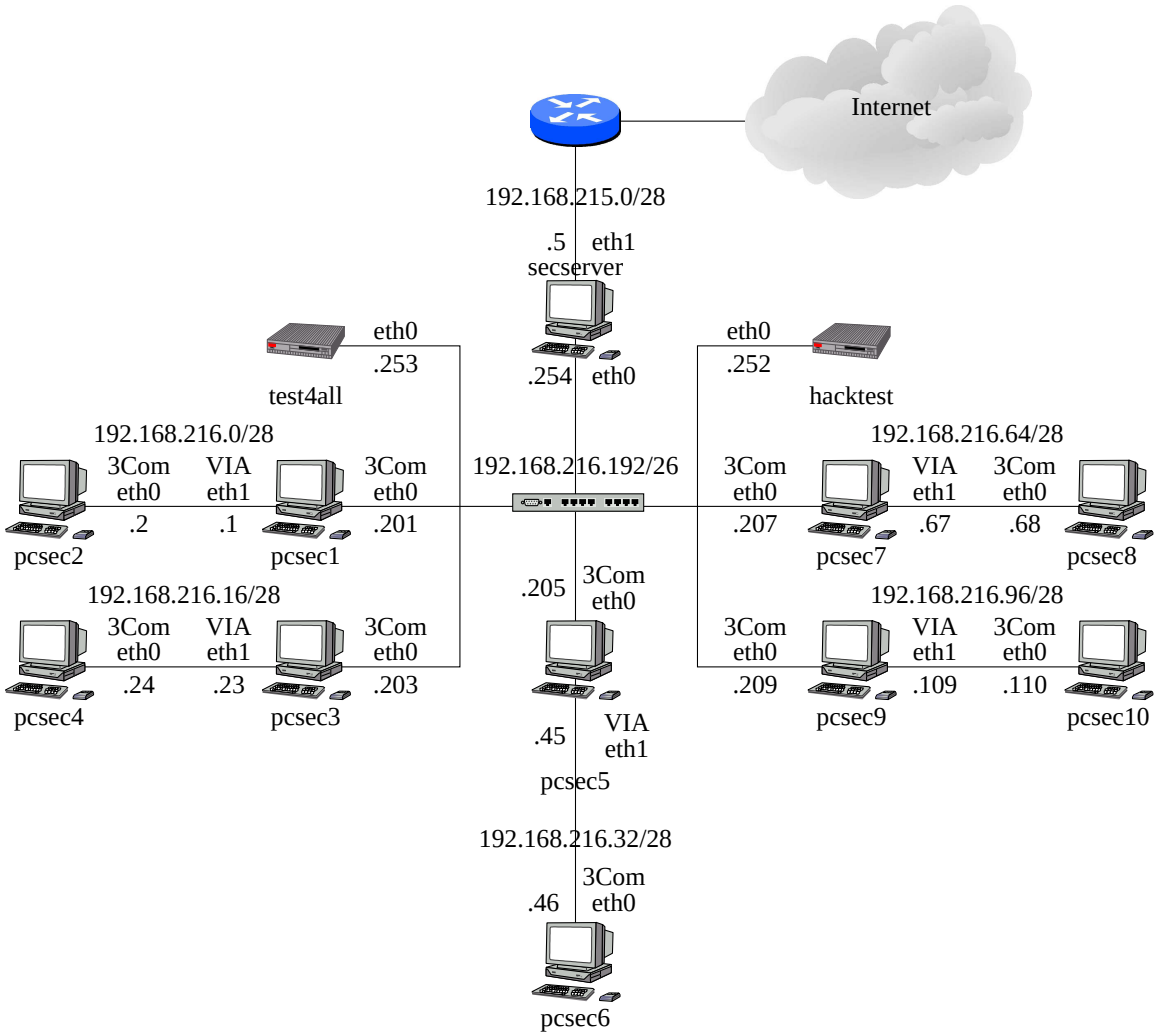


Abbildung 26: Der Versuchsaufbau für die weiteren Versuche des Praktikums

Für alle folgenden Versuche wird der Versuchsaufbau aus Abbildung 26 verwendet. Konfigurieren Sie die Umgebung auf die neue Topologie um. Verwenden Sie nun auch die Default-Route und fassen Sie ggf. Routen zusammen.
Bitte achten Sie darauf, daß die Interfaces `eth0` und `eth1` den richtigen Netzwerkkarten aus Abbildung 26 (3Com, VIA) zugeordnet werden. Diese Zuordnung weicht bei einigen Rechnern von der Zuordnung im ersten Versuchsaufbau (Abbildung 15) ab. Insbesondere werden die Realtec-Karten in der neuen Topologie nicht mehr benötigt. Die Änderungen an der Verkabelung werden vom Betreuer gemacht.

### 3.3.2 Statische Paketfilterung mit Netfilter

1. Stellen Sie sicher, daß die Standard-Firewall-Konfiguration Ihrer Distribution nicht aktiv ist und lassen Sie sich die Regeln aller Ketten anzeigen.

2. Erstellen Sie eine Firewall-Policy mit folgenden Eigenschaften:

   - Die Unix-Kommandos `ping <IP-Adresse>` und `traceroute <IP-Adresse>` sind für alle Rechner erlaubt und müssen nicht geloggt werden. Andere als die für diese Kommandos benötigten ICMP-Meldungen sollen nicht erlaubt sein.
   - Das Logging soll, falls in den folgenden Aufgaben verlangt, bei erlaubten TCP-Verbindungen immer so eingestellt werden, daß immer nur der Verbindungsaufbau einen Eintrag ins Systemlog erzeugt. Beim UDP-Logging ist, falls verlangt, jedes Paket mitzuprotokollieren.

   `pcsec2`, `pcsec4`, `pcsec6`, `pcsec8`, `pcsec10` (Rechner mit nur einer aktiven Netzwerkkarte):

   - Erlauben folgender Dienste vom eigenen Rechner aus zu allen anderen Rechnern:
     - Telnet, FTP, SSH, und SMTP mit Logging.
     - TCP-Port 3128 ohne Logging.
     - DNS-Abfragen mit Logging.
     - NTP-Abfragen ohne Logging.
   - Erlauben folgender eingehender Dienste:
     - Telnet mit Logging nur für Ihren Partnerrechner und den `secserver`
     - SSH für alle Rechner im Netz `192.168.216.0/24` mit Logging.
     - FTP ohne Logging für alle Rechner.

   `pcsec1`, `pcsec3`, `pcsec5`, `pcsec7`, `pcsec9` (Rechner mit zwei aktiven Netzwerkkarten):

   - Erlauben aller vom Firewall selbst ausgehenden Verbindungen bzw. Anfragen auf allen Ports zu allen anderen Rechnern im Netz. Alle TCP-Dienste außer Port 3128 sollen geloggt werden, UDP-Dienste nicht.
   - Erlauben von eingehenden Telnet- und SSH-Verbindungen für Ihren Partnerrechner und den `secserver`, mit Logging.
   - FTP, DNS- und NTP-Abfragen, SMTP und TCP-Port 3128 frei zwischen allen Rechnern im Netz `192.168.216.0/24` ohne Logging, TCP-Kommunikation zu anderen Netzen (Internet) nur mit Verbindungsaufbau aus `192.168.216.0/24`, mit Logging.

   Für alle Rechner gilt außerdem:

- Alle für die oben erlaubten Regeln nicht benötigten Pakete sind zu verwerfen. Dabei sollen alle Verbindungsanfragen unbeantwortet bleiben, nur Anfragen auf den auth/identd-Dienst müssen mit `Connection refused` beantwortet werden. Geloggt werden sollen bis auf Zugriffe auf den auth/identd-Dienst alle Zugriffe auf unerlaubte Ports, also auch bei TCP nicht nur Pakete zum Verbindungsaufbau.

3. Überprüfen Sie Ihre Firewall durch Austesten der benötigten Dienste und mit Hilfe eines Portscanners.

   Für die Konfiguration ist es ratsam, alle erforderlichen Befehle in ein Shellscript zu schreiben und dieses zur Aktivierung der Policy aufzurufen, siehe Abbildung 23.
   Legen Sie sich auch ein Script an, welches alle Firewall-Regeln entfernt und die Default-Policy auf ACCEPT zurücksetzt, um Dienste oder das Zusammenspiel mit den anderen Rechnern besser testen zu können. Natürlich gilt diese Vorgehensweise nur innerhalb der Praktikumsumgebung, in der realen Welt darf ein Firewall nicht einfach so geöffnet werden!

4. Richten Sie Ihren Rechner so ein, daß der Firewall beim Starten noch vor den Netzwerkkarten aktiviert wird.

5. Überprüfen Sie Ihre Firewall durch Austesten der benötigten Dienste und mit Hilfe eines Portscanners

### 3.3.3 Dynamische Paketfilterung mit Netfilter

1. Stellen Sie ihr statisches Regelwerk auf dynamische Paketfilterung um, die Funktionsweise Ihrer Firewall soll sich dabei nicht verändern. Erstellen Sie dafür eine neue Datei und löschen Sie die Konfiguration der statischen Filterung nicht!

2. Überprüfen Sie Ihre Firewall wieder durch Austesten der benötigten Dienste und mit Hilfe des Portscanners.