Netzwerktechnik-12

Christian Zahler

13 Internetanbindung von Firmennetzwerken

13.1 ICS *(Internet Connection Sharing)*

Wenn in einer Workgroup die Betriebssysteme

- **Windows 98 Second Edition**,
- **Windows ME**
- **Windows 2000 Professional** oder
- **Windows XP Home** bzw. **Windows XP Professional**

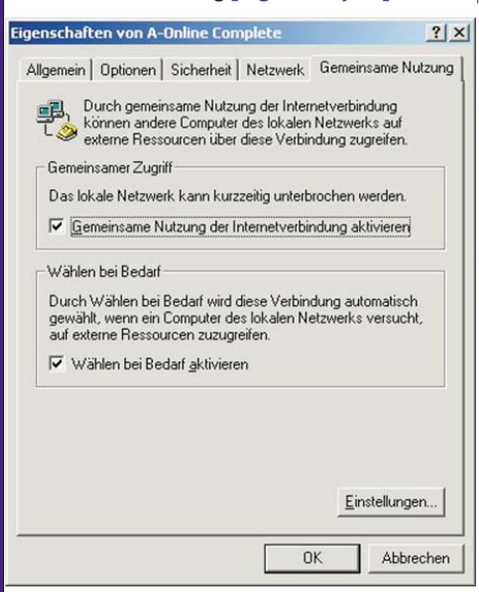
verwendet werden, dann besteht die Möglichkeit, einer bestehende Internetverbindung "freizugeben", sodass aller Mitglieder der Workgroup die auf einem PC eingerichtete Internetverbindung gemeinsam nutzen können.

Konsequenzen

- Der PC, auf dem die Internet-Freigabe eingerichet wird, erhält immer die statische IP-Adresse `192.168.0.1` mit der Subnetz-Maske `255.255.0.0`.
- Alle PCs im Netzwerk müssen IP-Adressen aus dem APIPA-Block verwenden (automatische private IP-Adressierung, d.h. `169.254.x.y`) und dürfen keine statischen IP-Einträge enthalten.
- **Die bestehende IP-Konfiguration des Netzwerks geht beim Einrichten einer Internet-Freigabe verloren! Das bedeutet, dass diese Methode für Firmennetze meist völlig ungeeignet ist!**

Durchführung

Zeigen Sie die aktuellen DFÜ-Verbindungen an (in Windows 2000 etwa ***Start*** – ***Einstellungen*** – ***Netzwerk- und DFÜ-Verbindungen***) und wählen Sie im Kontext Ihrer DFÜ-Internet-Verbindung ***[Eigenschaften]***:



In der Karteikarte ***„Gemeinsame Nutzung"*** (Windows XP: ***„Erweitert"***) aktivieren Sie dann das Kontrollkästchen ***„Gemeinsame Nutzung der Internetverbindung aktivieren"***.

13.2 Router

Abbildung: Cisco 800 (ISDN-Router)

Ein Router ist ein Gerät, welches in der Lage ist, Netzwerkadressen zu übersetzen bzw. Datenpakete nach vorgegebenen (programmierten) Gesetzmäßigkeiten weiterzuleiten. So könnte ein Router so programmiert sein, dass er die Schnittstelle zwischen zwei privaten Netzen mit den Netzwerknummern `192.168.43.x` und `192.168.54.x` darstellt.

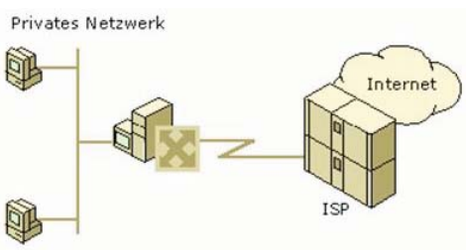
Dieser Router muss also in beiden Netzen erreichbar sein, wird also zwei IP-Adressen benötigen, zum Beispiel `192.168.43.254` und `192.168.54.254`. So ist der Router von beiden Netzwerken erreichbar; durch die eingestellten Vorgaben werden Datenpakete entweder weitergeleitet („geroutet") oder zurückgeschickt.

ISDN-Router sind in der Lage, ein kleines Netzwerk an eine gemeinsame ISDN-Leitung anzuschließen und so für alle PCs einen gemeinsamen Internetzugang zu ermöglichen.

Marktführer ist die Firma Cisco, andere bekannte Routerhersteller sind Nortel Networks oder Bay Networks.

13.2.1 Konfiguration einer weitergeleiteten Verbindung in Windows 2000-Netzwerken

Bei einer weitergeleiteten Verbindung dient der Windows 2000 Server-Computer als IP-Router, der die Pakete zwischen den SOHO-Hosts und den Internethosts weiterleitet.



Der Windows 2000-Router ist mit einem Netzwerkadapter für das im privaten Netzwerk verwendete Medium (z. B. Ethernet) sowie mit einem ISDN-Adapter oder einem analogen Modem konfiguriert. Sie können dabei eine Standleitung oder andere Technologien für permanente Verbindungen einsetzen, z. B. xDSL und Kabelmodems. In diesem Szenario wird jedoch die häufiger verwendete Konfiguration beschrieben, bei der eine Verbindung für Wählen bei Bedarf mit einem lokalen Internetdienstanbieter hergestellt wird.

Um eine weitergeleitete Verbindung mit dem Internet zu konfigurieren, muss in einem Netzwerk in einem kleinen Büro oder zu Hause Folgendes konfiguriert werden:

- Der Windows 2000-Router
- Andere Computer im Netzwerk in einem kleinen Büro oder zu Hause

Zum Konfigurieren des Windows 2000-Routers wird wie folgt vorgegangen.

1. Für das TCP/IP-Protokoll auf dem Windows 2000-Router für die Netzwerkschnittstelle in einem kleinen Büro oder zu Hause wird Folgendes festgelegt:
   - IP-Adresse (aus dem vom Internetdienstanbieter zugewiesenen Adressbereich)
   - Subnetzmaske (aus dem vom Internetdienstanbieter zugewiesenen Adressbereich)
   - DNS-Server (aus der vom Internetdienstanbieter zugewiesenen IP-Adresse)

   TCP/IP wird in der Komponente ***Netzwerk- und DFÜ-Verbindungen*** über die ***Eigenschaften*** des TCP/IP-Protokolls für die lokale Verbindung konfiguriert.

   Konfigurieren Sie keinen Standardgateway!

2. Der Routing- und RAS-Dienst wird installiert und aktiviert.

3. Auf dem DFÜ-Anschluss wird Routing aktiviert.

   Wenn Sie über eine ständige Verbindung mit dem Internet verfügen, die unter Windows 2000 als LAN-Schnittstelle angezeigt wird (z. B. DDS, T-Carrier, Frame Relay, ISDN, xDSL oder ein Kabelmodem) oder der Windows 2000-Computer keine direkte Verbindung mit dem Internet aufweist, sondern an einen anderen Router angeschlossen wird, fahren Sie mit Schritt 5 fort.

   Eine Schnittstelle für Wählen bei Bedarf wird erstellt, um eine Verbindung mit dem Internetdienstanbieter herzustellen.

4. Eine Schnittstelle für Wählen bei Bedarf wird erstellt, die für IP-Routing konfiguriert ist und die DFÜ-Ausstattung und -Anmeldeinformationen verwendet, die beim Wählen des Internetdienstanbieters verwendet werden.

5. Eine statische Standardroute unter Verwendung der Internetschnittstelle wird erstellt.

   Bei einer statischen Standardroute ist die Schnittstelle für Wählen bei Bedarf (bei DFÜ-Verbindungen) oder die LAN-Schnittstelle (bei permanenten Verbindungen oder Verbindungen über einen zwischengeschalteten Router) ausgewählt, die für die Verbindung mit dem Internet verwendet wird. Das Ziel ist `0.0.0.0`, und die Netzwerkmaske lautet `0.0.0.0`. Die IP-Adresse des Gateways kann auf der Schnittstelle für Wählen bei Bedarf nicht konfiguriert werden. Bei einer LAN-Schnittstelle, die eine Punkt-zu-Punkt-Verbindung mit dem Internetdienstanbieter darstellt, lautet die Adresse des Gateways `0.0.0.0`.

6. Multicastunterstützung wird konfiguriert (optional).

   So fügen Sie einem Netzwerk in einem kleinen Büro oder zu Hause Multicastunterstützung hinzu:

   - Das IGMP-Routingprotokoll wird hinzugefügt.
   - Auf der mit dem privaten Netzwerk verbundenen Schnittstelle wird der IGMP-Routermodus aktiviert.

- Auf der mit dem Internetdienstanbieter verbundenen Schnittstelle wird der IGMP-Proxymodus aktiviert.

Das TCP/IP-Protokoll auf dem Host in einem kleinen Büro oder zu Hause wird folgendermaßen konfiguriert:

- IP-Adresse (aus dem vom Internetdienstanbieter zugewiesenen Adressbereich)
- Subnetzmaske (aus dem vom Internetdienstanbieter zugewiesenen Adressbereich)
- Standardgateway (die IP-Adresse, die in einem kleinen Büro oder zu Hause dem Netzwerkadapter für den Windows 2000-Router zugewiesen ist)
- DNS-Server (aus der vom Internetdienstanbieter zugewiesenen IP-Adresse)

TCP/IP wird in der Komponente ***Netzwerk- und DFÜ-Verbindungen*** über die ***Eigenschaften*** des TCP/IP-Protokolls für die lokale Verbindung konfiguriert.

Anmerkung

- Bei der vorangegangenen Konfiguration von Hosts in einem kleinen Büro oder zu Hause wurde davon ausgegangen, dass TCP/IP manuell konfiguriert ist. Um TCP/IP für Hosts in einem kleinen Büro oder zu Hause automatisch zu konfigurieren, müssen Sie den DHCP-Server installieren und konfigurieren.
- Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig.

13.3 NAT *(Network Address Translation)*

Mit der Netzwerkadressübersetzung in Windows 2000 können Sie ein privates oder gewerblich genutztes Netzwerk für die gemeinsame Nutzung einer einzelnen Internetverbindung konfigurieren. Die Netzwerkadressübersetzung setzt sich aus folgenden Komponenten zusammen:

Übersetzungskomponente

Der Windows 2000-Router, auf dem die Netzwerkadressübersetzung aktiviert ist und der im Folgenden als NAT-Computer *(Network Address Translation)* bezeichnet wird, fungiert als Netzwerkadressübersetzer für die IP-Adressen und TCP/UDP-Anschlussnummern der Pakete, die zwischen dem privaten Netzwerk und dem Internet weitergeleitet werden.

Adresskomponente

Der NAT-Computer stellt den anderen Computern im privaten Netzwerk Konfigurationsdaten der IP-Adressen zur Verfügung. Bei der Adresskomponente handelt es sich um einen vereinfachten DHCP-Server, der eine IP-Adresse, eine Subnetzmaske, ein Standardgateway, die IP-Adresse eines DNS-Servers zuweist. Sie müssen die Computer im privaten Netzwerk als DHCP-Clients konfigurieren, um automatisch die IP-Konfiguration zu erhalten. Die standardmäßige TCP/IP-Konfiguration von Windows 2000-, Windows NT-, Windows 95- und Windows 98-Computern entspricht derjenigen eines DHCP-Clients.

Namensauflösungskomponente

Der NAT-Computer übernimmt für die anderen Computer im privaten Netzwerk die Funktion des DNS-Servers. Erhält der NAT-Computer Anforderungen zur Namensauflösung, leitet er diese an die entsprechenden DNS-Server im Internet weiter und sendet die Antworten an den jeweiligen Computer im privaten Netzwerk.

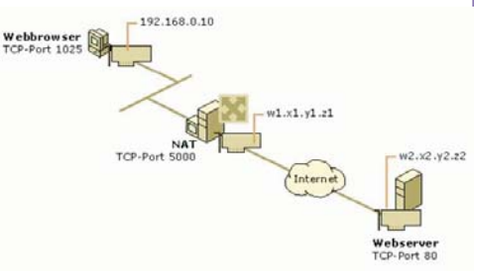
Beispiel

Angenommen, in einem kleinen Unternehmen wird die Netzwerkkennung `192.168.0.0` für das Intranet verwendet, und der Internetdienstanbieter hat dem Unternehmen die öffentliche Adresse `w1.x1.y1.z1` zugewiesen. Bei der Netzwerkadressübersetzung (NAT) werden alle privaten Adressen in `192.168.0.0` auf die IP-Adresse `w1.x1.y1.z1` gesetzt. Wenn mehrere private Adressen auf eine einzelne öffentliche Adresse gesetzt werden, verwendet NAT dynamisch ausgewählte TCP- und UDP-Ports, um die Hosts im Intranet voneinander zu unterscheiden.

Anmerkung

Die Adressen `w1.x1.y1.z1` und `w2.x2.y2.z2` stehen für gültige öffentliche IP-Adressen, die vom Internet Network Information Center (InterNIC) oder einem Internetdienstanbieter zugewiesen wurden.

- Die folgende Abbildung zeigt ein Beispiel, in dem NAT verwendet wird, um Verbindungen zwischen einem Intranet und dem Internet transparent herzustellen.



Wenn ein privater Anwender unter der Adresse `192.168.0.10` einen Webbrowser verwendet, um eine Verbindung mit dem Webserver unter der Adresse `w2.x2.y2.z2` herzustellen, wird ein IP-Paket mit den folgenden Informationen erstellt:

- IP-Zieladresse: `w2.x2.y2.z2`
- IP-Quelladresse: `192.168.0.10`
- Zielport: `TCP-Port 80`
- Quellport: `TCP-Port 1025`

Dieses IP-Paket wird dem NAT-Protokoll übergeben, das die Adressen des ausgehenden Pakets wie folgt ändert:

- IP-Zieladresse: `w2.x2.y2.z2`
- IP-Quelladresse: `w1.x1.y1.z1`
- Zielport: `TCP-Port 80`
- Quellport: `TCP-Port 5000`

Das NAT-Protokoll zeichnet die Zuordnung von {`192.168.0.10`, `TCP 1025`} zu {`w1.x1.y1.z1`, `TCP 5000`} in einer Tabelle auf.

Das so übersetzte IP-Paket wird über das Internet gesendet. Die Antwort wird zurückgesendet und vom NAT-Protokoll empfangen. Beim Empfang enthält das Paket die folgenden Informationen zur öffentlichen Adresse:

- IP-Zieladresse: `w1.x1.y1.z1`
- IP-Quelladresse: `w2.x2.y2.z2`
- Zielport: `TCP-Port 5000`
- Quellport: `TCP-Port 80`

Das NAT-Protokoll schlägt in der Übersetzungstabelle nach, setzt die öffentlichen Adressen wieder auf die privaten Adressen um und übermittelt das Datenpaket an den Computer unter der Adresse `192.168.0.10`. Das übermittelte Datenpaket enthält die folgenden Adressinformationen:

- IP-Zieladresse: `192.168.0.10`
- IP-Quelladresse: `w2.x2.y2.z2`
- Zielport: `TCP-Port 1025`
- Quellport: `TCP-Port 80`

Bei Datenpaketen, die vom NAT-Protokoll ausgehen, wird die IP-Quelladresse (eine private Adresse) auf die vom ISP zugewiesene Adresse (eine öffentliche Adresse) gesetzt, und die TCP- bzw. UDP-Portnummern werden auf andere TCP- bzw. UDP-Portnummern umgesetzt.

Bei Datenpaketen, die vom NAT-Protokoll empfangen werden, wird die IP-Zieladresse (eine öffentliche Adresse) auf die ursprüngliche Adresse im Intranet (eine private Adresse) gesetzt, und die TCP- bzw. UDP-Portnummern werden auf die ursprünglichen TCP- bzw. UDP-Portnummern zurückgesetzt.

Anmerkung

- Pakete, bei denen die IP-Adresse lediglich im IP-Header vermerkt ist, werden vom NAT-Protokoll ordnungsgemäß übersetzt. Pakete, bei denen die IP-Adresse in den IP-Nutzdaten enthalten ist, werden vom NAT-Protokoll möglicherweise nicht ordnungsgemäß übersetzt.

13.3.1 Konfiguration einer weitergeleiteten Verbindung in Windows 2000-Netzwerken

Bei einer übersetzten Verbindung dient der Windows 2000 Server-Computer als NAT (Netzwerkadressübersetzer), d. h., als IP-Router, der die Adressen der Pakete übersetzt, die zwischen den SOHO-Hosts und den Internethosts weitergeleitet werden.

Sie können die folgenden IP-Adressen des InterNIC als IDs für private IP-Netzwerke verwenden: `10.0.0.0` mit der Subnetzmaske `255.0.0.0`, `172.16.0.0` mit der Subnetzmaske `255.240.0.0` und `192.168.0.0` mit der Subnetzmaske `255.255.0.0`. In der Standardeinstellung wird bei der Netzwerkadressübersetzung die Netzwerkkennung `192.168.0.0` mit der Subnetzmaske `255.255.255.0` für das private Netzwerk verwendet.

So aktivieren Sie die Adressierung für die Netzwerkadressübersetzung:

1. Öffnen Sie Routing und RAS.
2. Klicken Sie in der Konsolenstruktur auf ***Verbindungsfreigabe*** (NAT).
   - Routing und RAS
   - Servername
   - IP-Routing
   - NAT
3. Klicken Sie mit der rechten Maustaste auf ***Verbindungsfreigabe*** (NAT), und klicken Sie auf ***Eigenschaften***.

4. Aktivieren Sie auf der Registerkarte ***Adressierung*** das Kontrollkästchen ***Automatische Adresszuweisung für Computer des privaten Netzwerks***.

5. Konfigurieren Sie ggf. unter ***Vom Netzwerk zuweisen*** und ***Mit Hilfe der Netzwerkmaske*** den Bereich der IP-Adressen, die den DHCP-Clients im privaten Netzwerk zugeordnet werden sollen.

6. Klicken Sie ggf. auf ***Ausschlüsse***, konfigurieren Sie die Adressen, die von der Zuordnung zu DHCP-Clients im privaten Netzwerk auszuschließen sind, und klicken Sie dann auf **OK**.

Wenn Sie eine öffentliche IP-Adresse verwenden, die Ihnen nicht vom InterNIC oder Ihrem Internetdienstanbieter zugewiesen wurde, verwenden Sie möglicherweise die IP-Netzwerkkennung einer anderen Organisation im Internet. Dies ist auch als ungültige oder überlappende IP-Adressierung bekannt. Wenn Sie überlappende IP-Adressen verwenden, können Sie die Internetressourcen, die sich an diesen Adressen befinden, nicht erreichen. Wenn Sie z. B. die Adresse `1.0.0.0` mit der Subnetzmaske `255.0.0.0` verwenden, können Sie die Internetressourcen der Organisation, die das Netzwerk `1.0.0.0` verwendet, nicht erreichen.

Sie können auch bestimmte IP-Adressen aus dem eingestellten Bereich ausschließen. Die ausgeschlossenen Adressen werden keinem Host im privaten Netzwerk zugewiesen.

Wenn Sie eine einzelne öffentliche IP-Adresse verwenden, die Ihnen vom Internetdienstanbieter zugewiesen wurde, müssen Sie keine Änderung an der IP-Adresskonfiguration vornehmen. Wenn Sie mehrere von Ihrem Internetdienstanbieter zugewiesene IP-Adressen verwenden, müssen Sie die NAT-Schnittstelle (Netzwerkadressübersetzung) auf den IP-Adressbereich einstellen. Sie sollten feststellen, ob sich der IP-Adressbereich, der Ihnen vom Internetdienstanbieter zugewiesen wurde, als Kombination aus IP-Adresse und Subnetzmaske ausdrücken lässt.

Wenn Ihnen eine Reihe von Adressen zugewiesen wurde, die eine 2er-Potenz darstellt (also 2, 4, 8, 16 usw.), können Sie diesen Bereich als Kombination einer einzelnen IP-Adresse und einer Subnetzmaske ausdrücken. Wenn Sie von Ihrem Internetdienstanbieter z. B. die öffentlichen IP-Adressen `200.100.100.212`, `200.100.100.213`, `200.100.100.214` und `200.100.100.215` erhalten haben, können Sie diese vier Adressen als `200.100.100.212` mit der Subnetzmaske `255.255.255.252` ausdrücken.

Wenn sich die IP-Adressen nicht als Kombination einer einzelnen IP-Adresse und einer Subnetzmaske ausdrücken lassen, können Sie sie als Bereich oder Reihe von Bereichen eingeben, indem Sie jeweils die erste und die letzte IP-Adresse angeben.

Beim typischen Einsatz der Netzwerkadressübersetzung (NAT) bei Anwendern zu Hause oder in einem kleineren Unternehmen sind lediglich ausgehende Verbindungen vom privaten Netzwerk in das öffentliche Netzwerk zulässig. Programme, z. B. Webbrowser, die im privaten Netzwerk ausgeführt werden, bauen Netzwerkverbindungen zu Ressourcen im Internet auf. Der gegenläufige Datenverkehr aus dem Internet kann die NAT überqueren, da die Verbindung aus dem privaten Netzwerk heraus initiiert wurde.

Wenn Sie den Zugriff auf Ressourcen im privaten Netzwerk aus dem Internet heraus freigeben möchten, führen Sie die folgenden Schritte durch:

- Richten Sie eine statische IP-Adresskonfiguration auf dem Ressourcenserver ein. Dies beinhaltet die IP-Adresse (aus dem Bereich der IP-Adressen, die der NAT-Computer zuweist), die Subnetzmaske (aus dem Bereich der IP-Adressen, die der NAT-Computer zuweist), den Standardgateway (die private IP-Adresse des NAT-Computers) und den DNS-Server (die private IP-Adresse des NAT-Computers).
- Schließen Sie die IP-Adresse des Ressourcenservers aus dem Bereich der IP-Adressen aus, die der NAT-Computer zuweisen kann.
- Konfigurieren Sie einen speziellen Port. Ein spezieller Port stellt eine statische Abbildung einer öffentlichen Adresse mit Portnummer auf eine private Adresse mit Portnummer dar. Mit einem speziellen Port wird eine eingehende Verbindung aus dem Internet auf eine bestimmte Adresse im privaten Netzwerk gelegt. Durch die Verwendung eines speziellen Ports können Sie einen Webserver im privaten Netzwerk erstellen, auf den aus dem Internet zugegriffen werden kann.

Möglicherweise müssen Anwendungen und Dienste konfiguriert werden, damit sie im Internet fehlerfrei funktionieren. Wenn z. B. die Anwender im Netzwerk in einem kleinen Büro oder zu Hause (auch bekannt als SOHO = *Small Office/Home Office*) das Spiel Diablo mit anderen Anwendern im Internet spielen möchten, muss die Netzwerkadressübersetzung für die Anwendung Diablo konfiguriert werden.

13.3.2 VPN-Verbindungen von einem SOHO-Netzwerk mit Netzwerkadressübersetzung

Wenn Sie mit Hilfe einer VPN-Verbindung (virtuelles privates Netzwerk) von einem SOHO-Netzwerk mit Netzwerkadressübersetzung auf ein privates Intranet zugreifen möchten, können Sie das *Point-to-Point-Tunneling-Protocol* (PPTP) verwenden und die VPN-Verbindung vom Host im SOHO-Netzwerk zum VPN-Server des privaten Intranets im Internet herstellen. Das NAT-Routingprotokoll verfügt über einen NAT-Editor für PPTP-Datenverkehr. Über einen NAT-Computer können keine Verbindungen mit dem *Layer-2-Tunneling-Protocol* (L2TP) auf *Internet Protocol Security* (IPSec) aufgebaut werden.

13.4 Proxy-Server

13.4.1 Grundlagen

Ein Proxy-Server ist eine Software, die auf dem PC installiert ist, der den Internet-Zugang besitzt. Es kann sich hier um einen Wählzugang (Modem, ISDN-Karte) oder um einen Standleitungszugang (ADSL, Kabelmodem, Powerline) handeln.

Diese Software erfüllt verschiedene Aufgaben:

- Sie sammelt die Anfragen von allen PCs im Netz, die auf den Proxy-Server zugreifen, und führt diese Anfragen durch. So wird bei Bedarf die Einwahl durchgeführt und nötige Webdateien heruntergeladen.
- Die heruntergeladenen Dateien werden zwischengespeichert; Vorteil: bei wiederholten Anfragen brauchen die Dateien nicht mehr vom Internet geholt werden, sondern befinden sich bereits lokal auf der Festplatte des Proxy-Servers und werden nur mehr von dort an den Client versandt.
- Leistungsfähige Proxy-Server enthalten auch einen Firewall, der vor Angriffen durch Hacker schützt.

13.4.2 Marktüberblick

Beispiele für Proxy Server, oft kombiniert mit NAT- und Firewall-Technologie::

- WinProxy (`www.ositis.com`)
- WinGate (`www.wingate.at`)
- JanaServer (`www.janaserver.de`)
- Microsoft ISA Server *(Internet Security and Access Server)*
- Squid (Linux-Produkt, kostenloser Download unter `www.squid-cache.org`)

13.4.3 Funktionsweise eines Proxy Servers

Beim WWW-Caching werden Dokumente, die von einem Browser angefordert werden, nicht direkt beim ursprünglichen Server geholt, sondern via einem so genannten Proxy-Server, der möglichst in der Nähe des Browsers installiert ist. Der Proxy-Server ist im Prinzip ein riesiges Reservoir an (kürzlich) angeforderten Dokumenten, welche vom Server in bezug auf ihre Aktualität verwaltet werden und allen Browsern zur Verfügung stehen, welche den Proxy-Server benutzen. Falls der Proxy-Server ein Dokument noch nicht kennt, oder die bekannte Version in bezug auf bestimmte Kriterien veraltet ist, so fordert er die aktuelle Version selbständig beim ursprünglichen Server an und schickt sie an den anfragenden Browser weiter. Damit kann der Netzwerkverkehr wesentlich reduziert werden, insbesondere dann, wenn viele Browser den gleichen Proxy-Server benutzen und/oder wenn dieselben Dokumente immer wieder von weit her geholt werden müssen (z.B. aus den USA). Der Betrieb eines Proxy-Servers ist somit nicht nur aus Kostengründen sehr vorteilhaft, er führt bei „bekannten“ Dokumenten auch zu wesentlich kürzeren Antwortzeiten.

Ein Proxy-Server (engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.

Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Web-Inhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internetinhalte. Der Proxy hat dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Web-Dokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf. Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC - allerdings abhängig vom je-

weiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen "unsichtbar" hinter ihm.

Vorteile eines Proxy-Servers

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus.

Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

13.4.4 Methode

Ein Proxy-Server hat im wesentlichen die folgenden Eigenschaften:

- Gegenüber einem Browser (Client) sieht er aus wie ein WWW-Server.
- Gegenüber einem WWW-Server sieht er aus wie ein Client.
- Er besitzt einen riesigen Speicher (cache), in dem er Dokumente speichert, die von den mit ihm verbundenen Browsern angefordert worden sind.
- Fordert ein Browser ein Dokument an, so prüft der Proxy-Server zuerst, ob er dieses Dokument bereits im Speicher hat. Falls ja, so prüft er nach, ob das Dokument in bezug auf bestimmte Kriterien noch aktuell ist. Ist es das, so schickt er es dem Browser direkt zurück, andernfalls schickt er dem ursprünglichen Server eine Anfrage, ob das Dokument in der Zwischenzeit modifiziert worden ist. Falls ja, so fordert er das neue Dokument an und schickt es an den Browser weiter, andernfalls schickt er dem Browser das bereits gespeicherte Dokument.
- Falls der Proxy-Server ein angefordertes Dokument noch nicht kennt, so gibt es mehrere Möglichkeiten:
  1. Er fordert es direkt beim ursprünglichen Server an.
  2. Er fordert es bei einem sog. parent-proxy an, einem Proxy-Server des Proxy-Servers.
  3. Er schickt eine Anfrage an einen sog. sibling-proxy (ein 'Geschwister'-proxy mit demselben parent), ob dieser eine aktuelle Version des Dokumentes hat. Falls ja, so holt er es dort, falls nein, so holt er es direkt beim ursprünglichen Server.
- Ein „reload“ des Browsers bewirkt immer, dass eine Rückfrage beim ursprünglichen Server (bzw. bei einem parent-proxy) erfolgt. Damit ist gewährleistet, dass der Proxy-Server immer die aktuelle Version des Dokumentes an den Browser zurückschickt.

13.4.5 Firewalls

Eine Firewall in Computern ist eine logische Vorrichtung, die ein privates Netz vor dem öffentlichen Teil (Internet) schützt.

Funktionsprinzip

Ein Computer mit installierter Routing-Software und 2 Schnittstellen (z.B. serielle Schnittstellen, Ethernet, Token Ring, usw.). Das Internet ist mit einer Schnittstelle verbunden, das zu schützende private Netz mit der anderen Schnittstelle. Jetzt, haben Sie zwei verschiedene Netze, die sich einen Computer teilen.

Der Firewall-Computer, von jetzt an »Firewall« genannt, kann beide Seiten erreichen, das geschützte private Netz und das Internet. Niemand aus dem geschützten Netz kann das Internet erreichen, und aus dem Internet kann niemand in das geschützte Netz.

Damit jemand das Internet vom geschützten Netz aus erreichen kann, muss er eine Telnet-Verbindung zum Firewall aufbauen und das Internet von dort aus benutzen. Entsprechend, um eine Verbindung vom Internet aus in das geschützte Netz zu bekommen, muss man auch durch den Firewall gehen.

Dieses stellt eine ausgezeichnete Sicherheit gegen Angriffe aus dem Internet dar. Falls jemand einen Angriff gegen das geschützte Netz machen will, muss er zuerst durch den Firewall gehen. Ein 2-stufiger Zugang zum gesicherten Netz ist resistent gegen Angriffe. Falls jemand das geschützte Netz über eine gemeinere Methode angreifen will, wie z.B. Mail-Bombe oder den berüchtigten »Internet Wurm«, werden sie nicht in der Lage sein das geschützte Netz zu erreichen. Dies ist ein ausgezeichneter Schutz.

Nachteile einer Firewall

Das größte Problem einer Firewall ist, dass er den Zugang zum Internet von der Innenseite kommend stark hemmt. Grundsätzlich reduziert er den Gebrauch des Internets dahingehend, als ob man nur einen „Dial-Up Shell Zugang“ haben würde. Sich in den Firewall einloggen zu müssen, um vollen Internet-Zugang zu haben ist eine starke Beeinschränkung.

Programme wie Netscape, die eine direkte Internet-Verbindung benötigen, werden hinter einem Firewall nicht arbeiten. Die Antwort zu diesem Problem hat ein Proxy-Server. Proxy-Server erlauben ein direktes Erreichen des Internets hinter einem Firewall.

Um die Möglichkeit, von einem Computer im geschützten Netz mit Netscape im Web zu lesen, anbieten zu können, setzt man einen Proxy-Server auf den Firewall auf. Der Proxy-Server würde so konfiguriert werden, dass ein Computer vom eigentlichen Port 80 des Firewalls zum Port 1080 des Proxy verbunden wird, um alle Verbindungen zu den richtigen Adressen umzuleiten.

Der große Vorteil von Proxy-Servern ist die absolute Sicherheit, wenn sie korrekt konfiguriert sind. Sie werden niemanden erlauben sie zu umgehen. Der Proxy-Server ist vor allem eine Sicherheitsvorrichtung. Seine Benutzung für einen Internet-Zugang mit begrenzten IP-Adressen wird viele Nachteile haben.

Ein Proxy-Server bietet Zugang von innerhalb des geschütztes Netzes zur Außenseite, aber die Innenseite wird völlig unerreichbar für die Außenseite bleiben. Dieses bedeutet keine Server-, Talk- oder Archie-Verbindungen, oder direkte Emails zu den Computern im geschützten Netz. Diese Nachteile können gering erscheinen, aber bedenken sie: Es liegt ein Dokument auf Ihrem Computer innerhalb eines per Firewall geschütztem Netzes.

FTP verursacht ein anderes Problem mit einem Proxy-Server. Beim Absenden des ls-Befehls, öffnet der FTP-Server einen Port auf der Kundenmaschine und übermittelt die Information. Ein Proxy-Server wird das nicht erlauben, somit arbeitet FTP nicht zuverlässig. Proxy-Server arbeiten langsam. Wegen dem größeren Protokollaufwandes werden fast alle anderen Mittel, um einen Internet-Zuganges zu bekommen, schneller sein.

Grundsätzlich, falls Sie ausreichend IP Adressen haben und ihnen macht die Sicherheit keine Sorgen, wird kein Firewall und/oder Proxy-Server benutzt. Falls Sie zu wenig IP Adressen haben und ihnen macht die Sicherheit keine Sorgen, wird man eher einen IP-Emulator benutzen wie Term, Slirp oder TIA. Diese Pakete arbeiten schneller, erlauben bessere Verbindungen, und stellen ein hochwertigen Zugang vom Internet zum geschützten Netz bereit.

Proxy-Server sind gut für jene Netzwerke mit vielen Hosts, welche einen transparenten Internetzugang wollen. Sie benötigen nur eine kleine Konfiguration und wenig Verwaltungsarbeit im laufenden Betrieb.

Funktion und Prinzip einer Firewall

Es gibt zwei Arten von Firewalls.

1. **IP** oder **Filter Firewall**s - die alles sperren bis auf ausgewählten Netzwerkverkehr

2. **Proxy-Server** - die einem die Netzwerkverbindung übernehmen

a) IP Filter Firewalls

Ein IP Filter Firewall arbeitet auf Paket-Ebene, er ist so konstruiert, dass er den Datenstrom kontrolliert auf Grund von Ursprung, Ziel, Port und Paket-Typ-Information die in jedem Daten-Paket enthalten sind.

Diese Art des Firewalls ist sehr sicher, aber es mangelt an einer brauchbaren Protokollierung. Er verbietet den Zugang zum privaten Netzwerk aber es wird nicht protokolliert wer auf das private Netzwerk zugreifen will oder wer vom privaten Netz Zugriff ins Internet haben will.

Filter Firewalls sind absolute Filter. Gibt man einem von außen den Zugriff auf das private Netz hat automatisch jeder Zugriff darauf.

In Linux ist *packet-filtering-software* seit Kernel 1.2.13 enthalten

b) Proxy Server

Proxy Server erlauben indirekten Zugang zum Internet durch den Firewall. Als Beispiel zur Funktion startet man einen Telnet zu einem System um von dort aus einen Telnet zu einem anderen zu starten. Nur mit einem Proxy-Server kann man diesen Vorgang automatisieren. Wenn man mit einer Client-Software einen connect zum Proxy-Server macht, startet der automatisch seine Client(Proxy)-Software und reicht die Daten durch.

Weil Proxy-Server ihre Kommunikation duplizieren, können sie alles mitprotokollieren was sie tun.

Der große Vorteil von Proxy-Server ist, sofern sie korrekt konfiguriert sind, dass sie absolut sicher sind. Sie erlauben keinem ein Durchkommen. Sie haben keine direkten IP-Routen.

13.4.6 Beispiel: Winproxy 4.0

WinProxy bietet Ihnen alles, was Sie benötigen, um alle Ihre Computer gleichzeitig mit Hilfe einer einzigen Internetverbindung und Ihrem gewohnten Internet Service Provider mit dem Internet zu verknüpfen. Außerdem enthält WinProxy innovative Funktionen, wie z. B. die integrierte Firewall, einen zentralisierten Virenschutz, Webseitenfilter und Anwenderprivilegien, die Ihnen vollständige Kontrolle über Ihren Internetzugang geben.

- Neue transparente Proxy-Technologie

WinProxy kombiniert die Einfachheit der Übersetzung von Netzwerkadressen mit der Flexibilität und Kontrolle eines Proxyservers. Damit erübrigen sich Neukonfigurierungen von Anwendungen oder die Installierung spezieller Software auf jedem Client Computer, während Sie, als Administrator, die Kontrolle behalten und den Internetzugang für das gesamte Netzwerk tatsächlich verbessern. Wegen der integrierten DNS und DHCP Server sind keine Netzwerkkonfigurierungen mehr nötig, und die Installierung ist selbst für Neulinge ein Kinderspiel.

- Einfache Installation

Mit der neuen transparenten Proxy-Technologie von WinProxy sind Sie innerhalb von Minuten startklar, denn sie verzichtet auf die Komplexität herkömmlicher Schemata, die geteilte Internetzugänge notwendig machten. Installieren Sie WinProxy einfach auf einem Ihrer Netzwerkcomputer. Der 'Intelligent Installation Wizard' kommt ohne Fachchinesisch aus, und überprüft Ihre Einstellungen für die Internetverbindung ganz automatisch.

- Zeitgleicher und transparenter Zugang

Mit WinProxy müssen sie weder spezielle Software noch individuelle Anwendungen auf jedem Computer installieren. Öffnen Sie einfach nur Ihren Browser oder eine andere Internetanwendung, und Sie sind automatisch im Internet. Und das funktioniert mit all Ihren Lieblingsanwendungen, einschließlich E-Mail, Chat, NetMeeting - und sogar Online-Spielen.

- Sichere Firewall und Anti-Virus Schutz

WinProxy schützt Ihr gesamtes Netzwerk vor Eindringlingen oder Viren aus dem Internet. Wählen Sie aus vordefinierten Sicherheitseinstellungen, oder konfigurieren Sie Ihre eigenen Einstellungen. Der eingebaute Anti-Virus Schutz(2) schützt Sie vor bösartigen Codes in E-Mail Anhängen und Downloads aus dem Internet, und schirmt Ihr Netzwerk vor infizierten Dateien ab.

- Blockieren Sie den Zugang zu unerwünschten Webseiten

WinProxys detaillierter Webseiten-Filter erlaubt Ihnen den Zugang zu Webseiten mit unerwünschten Inhalten zu unterbinden. Vordefinierte Listen werden regelmäßig aktualisiert und beinhalten Sex, Propaganda, kriminelle Absichten, Extremes oder Drogen.(3) Zweiundzwanzig weitere Kategorien können, für ein Maximum an Sicherheit, hinzugefügt werden. Zusätzlich können Sie, mit Hilfe einer „weißen Liste“ nur zu den von Ihnen festgelegten Seiten Zugang erlauben.

- Definierung von Anwenderprivilegien

Mit WinProxy können Sie kontrollieren, wer Zugang zum Internet hat. Limitierte Zugangszeiten können Sie von der Uhrzeit, vom Tag oder vom einzelnen Computer abhängig machen. Außerdem können Sie spezifische Anwendungen wie Browsing, Chat oder E-Mail zulassen.

- Schneller Seitenaufbau

Durch einen hochentwickelten netzwerkweiten Zwischenspeicher der HTTP und DNS hat jeder Anwender einen schnelleren Zugang zu häufig besuchten Seiten.

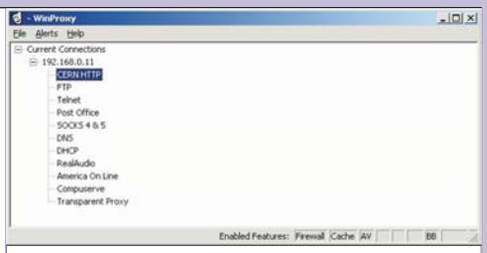
- Technische Hilfe

Selbst ein Experte benötigt von Zeit zu Zeit mal Hilfe. WinProxy beinhaltet deshalb Hilfe via E-Mail oder über seine umfassende Online-SupportBase (Hilfedatenbank).

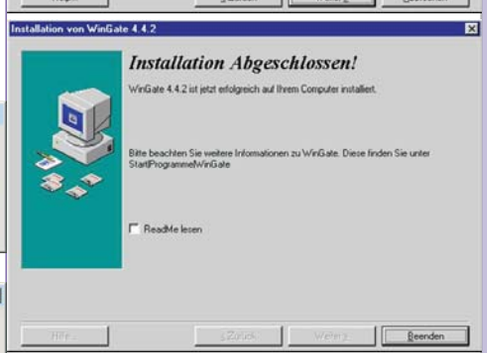
- Weitere Eigenschaften von WinProxy

WinProxy ist sparsam, da Sie nur noch einen Telefonanschluss, ein Modem, und ein Benutzerkonto benötigen.

- Funktioniert mit jedem ISP einschließlich AOL
- Windows 95/98/NT/2000/ME kompatibel
- Funktioniert mit Kabelanschluss, DSL, Modem, ISDN, Frame Relay, T1-T3, Funkverbindung
- Unterstützt praktisch alle PC-Netzwerke einschließlich Windows 95/98/NT/2000/Me, eingebaute Netzwerke und Netzwerke über Telefonlinien
- Benötigt keinen zusätzlichen Server
- Läuft automatisch im Hintergrund
- Unterstützt Mac und Unix/Linux Clients
- Internetspiele - unterstützt die meisten Onlinespiele
- Unterstützt alle bekannten E-Mail-Clients, einschließlich Eudora und Outlook, sowie mehrere Mail Server
- Bannerblockierung verhindert, dass sich unerwünschte Werbebanner aufbauen
- Erstellt oder beendet Internetverbindungen bei Bedarf automatisch
- Überwacht alle aktiven Internetzugänge in Echtzeit
- Protokolliert alle Verbindungen
- Unterstützt E-Mail und Webserver, die sich hinter der Firewall befinden.
- Proxy Cascading und verzeichnete Port-Unterstützung



13.4.7 Beispiel: Installation von WinGate 4.4 als Proxyserver



13.4.8 Beispiel: squid für Linux

Vorteile von Squid

- Kürzere Wartezeit beim Download
- Geldersparnis (Telefon, Volumengebühr)
- Bandbreitenschonung

Die Zeitersparnis kommt dadurch zustande, dass Daten, die sich im Cache befinden, rasch über die schnellen Intranetleitungen transportiert werden, anstelle über langsame Internetleitungen. Weiterhin kann die zu übertragende Datenmenge zu überlasteten Servern minimiert werden. Hier bringt z.B. bei Newsseiten Erleichterung, dass die meist recht vielen grafischen Icons sich lange nicht ändern, direkt aus dem Cache kommen, und so nur Text übrigbleibt. So ist man in der Lage, nicht nur sich selbst und seinem Geldbeutel einen Gefallen zu tun, sondern z.B auch den anderen Mitgliedern des Hausnetzes, die um jedes Byte, das mehr auf der Telefonleitung frei ist, froh sein werden.

- Beseitigung von Netscape-Hängern

Viele von Ihnen ärgern bestimmt die häufigen Aussetzer von Netscape, bei denen alle Fenster des Browsers betroffen sind. Sobald eine DNS-Abfrage länger dauert, lässt sich der Seiteninhalt nicht mehr scrollen und wird auch nicht mehr aktualisiert. Dies führt dazu, dass man während der manchmal recht langen Zeit gar nichts mit Netscape anfangen kann, da es nicht einmal möglich ist, bereits fertig dargestellte Seiten zu lesen. Zumindest wenn man mehrere Fenster übereinander, iconisiert oder auf einer anderen Seite des Windowmanager liegen hat. Hier kann Squid weiterhelfen, denn Netscape stellt seine Anfrage nun an den lokal gut zu erreichenden Squid-Server und ist von der DNS-Problematik befreit.

- Freischaltung bestimmter Rechner zu genau definierten Zeiten

Squid verfügt über sogenannte *"Access Lists"*, kurz **acl**. In diese kann man Rechner, Subnetze, Protokolle, Ports, URLs etc. aufnehmen. Sobald eine acl definiert ist, kann diese benutzt werden, um den Zugang zu ermöglichen oder zu sperren. So ist es in einer Firma z.B. sehr einfach zu realisieren, dass die Rechner aller Mitarbeiter in der Mittagspause surfen können. Während der Arbeitszeit hingegen bleibt der Zugang denen vorbehalten, die ihn benötigen. Hierzu wird neben dem Webcache noch ein Firewall gebraucht der verhindert, dass alle Rechner freien Zugang in und aus dem Netz heraus besitzen.

Durch die Möglichkeit komplette URLs und reguläre Ausdrücke in acl-Listen aufzunehmen, können komplette WWW-Server gesperrt werden oder solche bei denen bestimmte Schlüsselwörter im URL auftreten.

- Nutzung eines Wählzugangs mit einer einigen IP-Nummer zum Surfen mit mehreren Rechnern

Eine weiter schöne Einsatzmöglichkeit liegt darin, ohne sich mit IP-Masquerading befassen zu müssen, weiteren Rechnern den Zugang zum WWW bereitzustellen. Hierzu wird Squid einfach auf dem Rechner installiert der für den Verbindungsaufbau zuständig ist. Die Konfiguration für Squid ändert sich dadurch nicht.

- Einfache Überprüfung der heruntergeladenen Inhalte möglich

Durch die von Squid erstellten Logdateien lassen sich mittels diverser Skripte Übersichten erstellen, die einige interessante Statistiken erfassen. So können alle WWW-Server, auf die zugegriffen wurde, mit Anzahl, Menge und Art der Abfragen eingesehen werden. Eine aktuelle Liste dieser Skripte kann man auf der offiziellen Squid Webseite *http://squid.nlanr.net/* finden. Sie sind zumeist von Anwendern für private Zwecke geschrieben worden, daher nicht in das Squid-Paket integriert und müssen "von Hand" installiert werden.

- Zurückverfolgung der Übertragungen zu den einzelnen Rechnern möglich
- Anonymisieren der User nach innen und außen hin möglich

Sobald Squid WWW-Anfragen der User weiterleitet, wird ein *"forwarded for xyz"* in den HTTP-Header eingefügt. Diese Informationen kann der WWW-Server speichern und verarbeiten. Um zu verhindern, dass Nutzerprofile angelegt werden, kann die Konfiguration so umgestellt werden, dass diese Informationen nicht verschickt werden bzw. einen fest definierten Wert erhalten. Je nach Konfiguration speichert Squid in seinen eigenen Logdateien aber noch, für welche Rechner er die Daten herausgegeben hat. Dies kann für alle diejenigen wünschenswert sein, die auf eine Kontrolle bzw. einen Beleg angewiesen sind. Dabei sollten aber alle Aspekte des Datenschutzes beachtet werden. Falls man andererseits die Privatssphäre seiner Benutzer schützen will, kann dies durch eine entsprechende Konfiguration auch gewährleistet werden.

Nachteile von Squid

- Eventuell kommt es zur Auslieferung nicht mehr aktueller Daten

Squid teilt gespeicherte Daten in die zwei Klassen FRESH und STALE ein. Diese Einteilung wird mittels mehrere Regeln und dem Zeitpunkt der Übertragung sowie des Alters des Dokuments bestimmt. Solange ein Objekt FRESH ist, wird es bei einer erneuten Anfrage sofort aus dem Cache ausgeliefert. Ansonsten werden verschiedene Maßnahmen eingeleitet um zu überprüfen, ob das gespeicherte Objekt noch aktuell ist. Trotzdem kann es vorkommen, dass Objekte ausgeliefert werden, die nicht mehr dem letzten Stand entsprechen. Dies tritt vor allem bei Seiten ein, die sich täglich oder stündlich ändern. Wenn man den Verdacht hat, dass die dargestellte Seite nicht aktuell ist sollte man in Netscape, falls ein Reload erfolglos ist, mittels Shift-Reload einen neuen kompletten Download erzwingen.

- Eventuelle Probleme mit nur über Links zugänglichen Daten

Leider kann mit Shift-Reload kein neues Laden eines Links erzwungen werden. Diese Designschwäche des Browsers kann zu ärgerlichen Ergebnissen führen. Stellen Sie sich einmal vor, Sie wollen eine Liveübertragung eines Fußballspieles per Realaudio verfolgen. Die dazu nötige `.ra`-Datei ist über einen Link zugänglich und beim Anklicken wird das Realvideo-Plug-in aktiv. Weiterhin befindet sich vor der eigentlichen Übertragung ein Ankündigungstrailer unter diesem Link. Ist man nun etwas früh, hat man folgendes Problem: Der Trailer befindet sich im Cache und ist FRESH. Daher wird dieser, sobald man wieder auf den Link klickt, vom Cache ausgeliefert, obwohl die Übertragung jetzt läuft. Da man kein neues Laden über den Browser erzwingen kann, befindet man sich in der Situation, dass es nur möglich ist die Übertragung zu verfolgen, wenn man für alle Fenster des Browsers den Cache abschaltet. Um dem Ganzen aus dem Weg zu gehen, muss man dem Cache mitteilen, welche Dateitypen er nicht cachen soll. In der Standardkonfiguration befinden sich nur cgi und ? in dieser Liste. Sie sollte also nach Bedarf um all die Dateitypen erweitert werden, die nur per Links zugänglich sind.

Systemvoraussetzungen

Für den Betrieb von Squid bieten sich alte Rechner wie ein 486er geradezu an. Mit wenigen Mitteln kann man aus seinem alten Rechner ein schönes Gateway machen, das gleichzeitg für Verbindungsaufbau, Firewall und den Webcache zuständig ist. Man sollte nur darauf achten, dass dem Rechner genügend Hauptspeicher zur Verfügung steht. In diesem Fall fehlen eventuell nur noch ein oder zwei Netzwerkkarten, die es heute aber auch schon sehr günstig gibt.

Wenn möglich, sollte man dem Rechner zwei Festplatten spendieren, eine für das System und die andere auf der die Daten von Squid liegen. Dies sollte unbedingt der Fall sein, wenn der Rechner häufig swapt, weil er zuwenig Hauptspeicher besitzt. Squid läuft auf quasi allen Unix-Betriebssystemen. Auf der Tagungs-CD-ROM ist ein Binary-RPM für Red Hat 5.2 enthalten, das Sie recht einfach als root mittels `rpm -i dateiname` installieren können. In der Delix DLD-Distribution, die sich auf der CD-ROM zum LinuxTag '99 befindet, ist das Paket leider nur in einer etwas älteren Version verfügbar. Für die Betreiber von anderen oder älteren Systemen ist auch ein Source-RPM vorhanden. Mit dessen Hilfe können Sie ein für Ihr System passendes Binary-RPM erzeugen.

Wichtigste Konfigurationsoptionen

Im folgenden Abschnitt finden Sie die wichtigsten Konfigurationsoptionen aus der Datei `etc/squid.conf`, mit deren Hilfe Sie Ihren Cache grundlegend konfigurieren können. Die folgenden Optionen sind dem Konfigurationsfile der Version 2.1 entnommen.

Dieser Text ist aus Platzgründen in die Webversion verlagert worden.

13.5 Quellen

www.tecchannel.de

http://www.zdnet.de/technik/artikel/swp/200006/proxy_01-wc.html

Squid-Konfiguration

```
# NETWORK OPTIONS
# -----------------------------------------------------------------------------
#  TAG: http_port
#http_port 3128
Mittels des http_port stellen Sie ein, unter welcher Portnummer auf Ihrem Rechner Squid zu erreichen
ist (siehe Einführung).
# OPTIONS WHICH AFFECT THE CACHE SIZE
# -----------------------------------------------------------------------------
#  TAG: cache_mem       (bytes)
#cache_mem  8 MB
#  TAG: maximum_object_size     (bytes)
#maximum_object_size 4096 KB
Durch cache_mem wird festgelegt, wieviel Speicher für In-Transit-Objekte zur Verfügung steht. Dies
sind alle Daten, die in Übertragung begriffen sind. Zeitweilig kann diese Größe überschritten werden,
falls z.B eine tar.gz-Datei heruntergeladen wird, die größer als der cache_mem-Wert ist.
maximum_object_size legt die maximal Größe einer Datei fest, die noch im Cache gspeichert wird. Beide
Optionen sollten an Bedarf und Systemressourcen angepasst werden. Es macht z.B keinen Sinn, den
gesamten Hauptspeicher als Größe anzugeben, zumal wenn Squid auf dem Arbeitsrechner läuft.
# LOGFILE PATHNAMES AND CACHE DIRECTORIES
# -----------------------------------------------------------------------------
#  TAG: cache_dir
#cache_dir /usr/local/squid/cache 100 16 256
#  TAG: cache_access_log
#cache_access_log /usr/local/squid/logs/access.log
#  TAG: cache_log
#cache_log /usr/local/squid/logs/cache.log
#  TAG: cache_store_log
#cache_store_log /usr/local/squid/logs/store.log
#  TAG: cache_swap_log
#cache_swap_log
#  TAG: pid_filename
#pid_filename /usr/local/squid/logs/squid.pid
Falls eine extra Festplatte/Partition für die Daten zur Verfügung steht, empfiehlt es sich, die
Logdateien ebenfalls dort abzulegen. Dementsprechend müssen die Pfade angepasst werden, z.B.
/mnt/proxy/....
Die Datei swap.state darf unter keinen Umständen gelöscht werden, da darin die Informationen
gespeichert werden, wo auf der Festplatte die Daten des Caches abgelegt sind. Diese Datei wird beim
Neustart von Squid verwendet, um wieder auf die gespeicherten Daten zugreifen zu können. In den
anderen Datein sind Informationen, Zugriffe und Status verzeichnet.
#  TAG: ident_lookup    on|off
#ident_lookup off
Mittels dieser Option ist es möglich, eine Abfrage des Nutzernamens beim Client durchzuführen und im
Log zu speichern.
#  TAG: client_netmask
#client_netmask 255.255.255.255
Um einen entsprechenden Datenschutz für die Benutzer im Log zu erreichen, kann man die IP-Nummern der
Rechner ähnlich wie Telefonnummern auf einer Telekomrechnung um beliebige Stellen kürzen. Mittels
client_netmask 255.255.255.0
erreicht man z.B., dass aus 194.162.83.24 194.162.83.0 wird und die letzten acht Bit der IP-Adresse
verloren gehen. Die wahre IP-Nummer wird dabei einfach mit client_netmask durch die logische
und-Funktion verknüpft, bevor sie im Log gespeichert wird.
# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
# -----------------------------------------------------------------------------
#  TAG: dns_children
#dns_children 5
Die dns_children sind dazu da, die Nameserverabfragen zu übernehmen. Bei normaler Benutzung kann man
diese Option unverändert lassen. Falls der Cache dafür gedacht ist vielen Leuten zu dienen, und diese
über eine langsame Leitung angebunden sind, sollte die Anzahl eventuell erhöht werden. Die
Programmierer empfehlen für einen sehr stark ausgelasteten Cache mindestens 10. Der Maximalwert
beträgt 32. Man sollte aber bedenken, dass jeder weitere DNS-Prozess etwa 100kB Hauptspeicher belegt.
# OPTIONS FOR TUNING THE CACHE
# -----------------------------------------------------------------------------
#  TAG: reference_age
#reference_age 1 month
Beim Aufräumen des Caches werden alle Objekte entfernt, die ihr maximales Alter erreicht haben. Wenn
reference_age auf einen Monat eingestellt ist, werden alle Objekte entfernt, auf die seit einem Monat
nicht mehr zugegriffen wurde.
#  TAG: quick_abort_min (KB)
#  TAG: quick_abort_max (KB)
#  TAG: quick_abort_pct (percent)
#quick_abort_min 16 KB
#quick_abort_max 16 KB
#quick_abort_pct 95
Squid ist in der Lage, Dateien, deren Übertragung er begonnen hat, auch nach dem Beenden bzw. Stoppen
des Browsers durch den Benutzer fertig zu laden, falls sie bestimmten Kriterien genügen. Falls
weniger als quick_abort_min Kilobyte von der Übertragung übrig bleiben, wird diese fortgesetzt. Wenn
mehr als quick_abort_max Kilobyte zu laden sind, wird der Transfer abgebrochen. Die letzte Bedingung
quick_abort_pct legt fest, wieviel Prozent der Übertragung abgeschlossen sein müssen, um diese
fortzusetzen.
Die quick_abort-Funktionalität hat Ihre Stärken und Schwächen. Durch die fortgesetzte Übertragung
kann es, vor allem auf langsamen Leitungen wie Wählverbindungen, zu Engpässen und starker
Verlängerung der Transferzeiten kommen. Andererseits sind dann vollständige Daten im Cache auch für
andere Benutzer abrufbar. Der Standardnutzer sollte die quick_abort-Funktion abstellen. Dies
geschieht durch
quick_abort_min 0 KB
quick_abort_max 0 KB
quick_abort_pct 100
# TIMEOUTS
# -----------------------------------------------------------------------------
#  TAG: request_timeout
#request_timeout 30 seconds
Bei stark ausgelasteten Leitungen bietet es sich an, den Timeout nach Bedarf anzupassen.
# ACCESS CONTROLS
# -----------------------------------------------------------------------------
#  TAG: acl
#Defaults:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 21 443 563 70 210 1025-65535
acl CONNECT method CONNECT
#  TAG: http_access
#Default configuration:
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access deny all
Access Control Lists, kurz acl, werden nach folgendem Syntax definiert:
acl aclname acltyp string1 ...
acl aclname acltyp datei ...
In einer Datei sollte nur eine Regel pro Zeile eingetragen werden. Die unterschiedlichen acltypen
sind:
src
Fasst Herkunfts-IP-Adressen zusammen.
IP-Adresse/Netzmaske ... (Client-IP-Adresse)
Addr1-Addr2/Netzmaske ... (Bereich von Adressen)
dst
Fasst Ziel-IP-Adressen zusammen.
srcdomain
Herkunftsdomain.
dstdomain
Zieldomain.
srcdom_regex
Regulärer Ausdruck angewendet auf den Client.
dstdom_regex
Regulärer Ausdruck angewendet auf den Server.
url_regex
Regulärer Ausdruck, der auf den ganzen URL angewendet wird.
urlpath_regex
Regulärer Ausdruck, der auf den Pfad des URL angewendet wird.
time
Tages und Zeitbereichsangabe Tag h1:min1-h2:min2. Die erste Zeitangabe muss kleiner als die zweite
sein. Tag:
M
Montag
T
Dienstag
W
Mittwoch
H
Donnerstag
F
Freitag
A
Samstag
S
Sonntag
port
Portnummern
proto
Protokoll
method
Methoden wie GET, POST, ...
browser
regular expression
ident
Benutzername
http_access erlaubt oder sperrt den Zugriff auf Squid durch Access-Lists. Zugriff auf den HTTP-Port:
http_access allow|deny [!]aclname
Wenn keine http_access-Zeile vorhanden ist, wird die Anfrage grundsätzlich erlaubt. Wenn keine
http_access-Zeile auf einen Anfrage angewendet werden kann, wird das Gegenteil der letzten Regel in
der Liste angewendet. Die Regeln werden eine nach der anderen von oben nach unten abgearbeitet, bis
eine Regel zutrifft. Danach folgende Regeln werden nicht mehr berücksichtigt. Innerhalb einer acl
sind die Elemente mit oder und bei http_access mit und verknüpft.
Nehmen wir einmal an, der Zugang zum WWW soll für zwei Benutzergruppen reglementiert werden.
acl standard src 194.246.68.1-194.246.68.100/255.255.255. 194.246.68.102/255.255.255.255
acl privilegiert src 194.246.68.101/255.255.255.255 194.246.68.103/255.255.255.255
acl Mittagspause 12:00-13:00
http_access allow Mittagspause standard
http_access deny standard
http_access allow privilegiert
http_access deny all
Mit dieser Konfiguration werden die Standard-Nutzer nur zur Mittagspause freigeschaltet, während die
privilegierten Nutzer jederzeit Zugriff besitzen. Alle diejenigen IP-Nummern, die durch die Listen
nicht abgedeckt werden, haben keinen Zugriff.
# ADMINISTRATIVE PARAMETERS
# -----------------------------------------------------------------------------
#  TAG: cache_mgr
#cache_mgr webmaster
Hier muss die E-Mail-Adresse desjenigen eingetragen werden, der die Administration von Squid
übernommen hat.
# MISCELLANEOUS
# -----------------------------------------------------------------------------
#  TAG: dns_testnames
#dns_testnames netscape.com internic.net nlanr.net microsoft.com
Mit den eingetragenen Domains wird die DNS-Abfrage überprüft. Sobald der erste erfolgreiche
DNS-Lookup gelingt, wird der Test erfolgreich abgebrochen. Ansonsten wird nach einer gewissen Zeit
Squid beendet (z.B falls die Leitung gerade nicht aufgebaut ist). Um den DNS-Test zu unterbinden,
muss Squid mit squid -D gestartet werden.
#  TAG: append_domain
#append_domain .yourdomain.com
append_domain dient der Bequemlichkeit und ermöglicht es im Browser Rechnernamen des lokalen Netzes
ohne Domainnamen anzugeben. Squid ergänzt diese automatisch um die Zeichenkette in append_domain.
Also z.B append_domain .unix-ag.uni-kl.de. Aus http://sushi wird somit
http://sushi.unix-ag.uni-kl.de.
#  TAG: memory_pools    on|off
#memory_pools on
Wenn memory_pools aktiviert ist, behält Squid ungenutzten zugewiesenen Speicher für zukünftigen
Gebrauch, anstatt ihn wieder freizugeben. Wenn der Rechner über wenig Speicher verfügt, sollte man
memory_pools abschalten.
#  TAG: forwarded_for   on|off
#forwarded_for on
Standardmäßig leitet Squid die IP-Nummer oder den Namen eines Rechners, für den eine Anfrage
bearbeitet wird, zum WWW-Server weiter.
forwarded_for off
#  TAG: http_anonymizer
#http_anonymizer off
Mittels http_anonymizer lässt sich konfigurieren, wieviele HTTP-Header gefiltert werden. Es gibt die
drei Einstellungen off, standard und paranoid. Mit standard werden die wichtigsten Header
unterdrückt, mit paranoid hingegen fast alle.
Unter Version 2.2 wurde diese Option dahingehend verändert, dass nun die einzelnen Header, die
erlaubt oder unterdrückt werden sollen, direkt angegeben werden können.
Squid starten
Nach den Änderungen an der Datei muss der Squid neu gestartet werden sofern er schon läuft. Dies
geschieht am einfachsten mit dem Befehl /sbin/init.d/squid restart.
Damit Squid bei jedem Start Ihres Linux-Rechners automatisch gestartet wird, setzen Sie in der Datei
/etc/rc.config den Wert von START_SQUID auf yes.
Logdateien rotieren
Um eine Rotation der Logdateien auszuführen, können Sie squid -k rotate verwenden.
Squid rekonfigurieren
Nach einer Änderung an der Konfiguration ist es möglich mittels squid -k reconfigure ein Neueinlesen
einzuleiten.
Squid beenden
Benutzen Sie einfach squid -k shutdown, um Squid nach ungefähr einer halben Minute terminieren zu
lassen.
```