Ein intensiver Dialog mit dem Anwender und eine Inspektion der örtlichen Gegebenheiten sind für eine sinnvolle Netzwerkplanung unverzichtbar. Denn: Jedes Netz ist anders.

Sind die in aller Kürze oben genannten *strategischen* Rahmenbedingungen geklärt, folgt die *taktische* Klein- und Routinearbeit:

- Erstellen von Plänen
- Bestimmung von Längenmetern und Stückzahlen
- Kennzeichnung von Dosen und Patchfeldern
- etc.

Ein Großteil dieser Routinearbeiten kann heute von spezieller Netzwerkplanungssoftware übernommen werden.

1.7.2.2 Administration

Die Administration umfasst die folgenden Tätigkeitsbereiche:

- Bestandsführung der Hard- und Software inklusive Beschaffung und Aussonderung
- Betriebsmittelverwaltung (z. B. Drucker)
- Benutzerverwaltung
- Aufrechterhaltung der Verfügbarkeit (Störungsanalyse und -beseitigung)
- Aufrechterhaltung der übrigen Informationssicherheit (Vertraulichkeit, Unverfälschtheit)

Die ersten beiden Punkte dieser Liste werden hier nicht weiter ausgeführt. Die Benutzerverwaltung ist sehr betriebssystemspezifisch, deswegen wird auf die entsprechenden Teile des Kapitels 2 verwiesen.

Aufrechterhaltung der Verfügbarkeit

Trotz Sorgfalt bei Installation und Konfiguration zur Vorbeugung von Störungen können diese auftreten. Ziel der Netzadministration sollte es diesbezüglich sein,

- es zum einen **vorausschauend** gar nicht erst bis zur Störung kommen zu lassen, denn viele als Störung zu bezeichnende Betriebszustände eines Netzes sind nur die Endpunkte einer Entwicklung über einen längeren Zeitraum,
- und zum anderen Sofortmaßnahmen bereitzuhalten, die eine spontane Störung binnen Kurzem beseitigen oder bis zur endgültigen Beseitigung überbrücken.

Zu den vorausschauenden Maßnahmen gehören:

- Regelmäßig aktualisierter **Virenschutz**
- Regelmäßige **Datensicherung** mit Rotation und Aussonderung überalterter Datenträger
- Regelmäßige **Software-Updates**
- Regelmäßige Inspektion der **Protokolldateien** (Logfiles) der Serverprozesse
- Regelmäßige Überprüfung des **freien Plattenplatzes** und Abschätzung des Wachstumsverhaltens der Belegung

- Regelmäßige Überprüfung der **Prozessorauslastung** auf den Servermaschinen und Abschätzung des Wachstumsverhaltens der Auslastung
- Ständige Überwachung des **Traffics** (Datenverkehr im Netz) auf Lastspitzen und Engpässe

Manche dieser Tätigkeiten sind entweder nur schwer oder, wie der letzte Punkt, fast gar nicht „manuell" zu leisten. Dies gilt insbesondere für große (viele Komponenten) und räumlich ausgedehnte Netze (Hybridnetze: siehe auch Kap. 3, VPN). Dazu werden Netzwerk-Management-Systeme eingesetzt.

Bei spontanen Störungen setzt der Einsatz von Sofortmaßnahmen deren **Vorbereitung** voraus.

Zu den Sofortmaßnahmen gehören beispielsweise:

- **Restauration** (Wiedereinspielen von Datensicherungen)
- Automatische **Reaktivierung von Ressourcen**, wie z. B. in Bild 1.170c dargestellt oder mit Stand-by-Komponenten (redundante Platten und Netzteile)
- **Konfigurationsänderung**, wie im folgenden Beispiel beschrieben

Beispiel zur Konfigurationsänderung

In einem lokalen Beispielnetz hat der HTTP-Traffic den bei Weitem größten Anteil. Daher wird es über zwei HTTP-Proxies ans Internet angebunden (Bild 1.183).

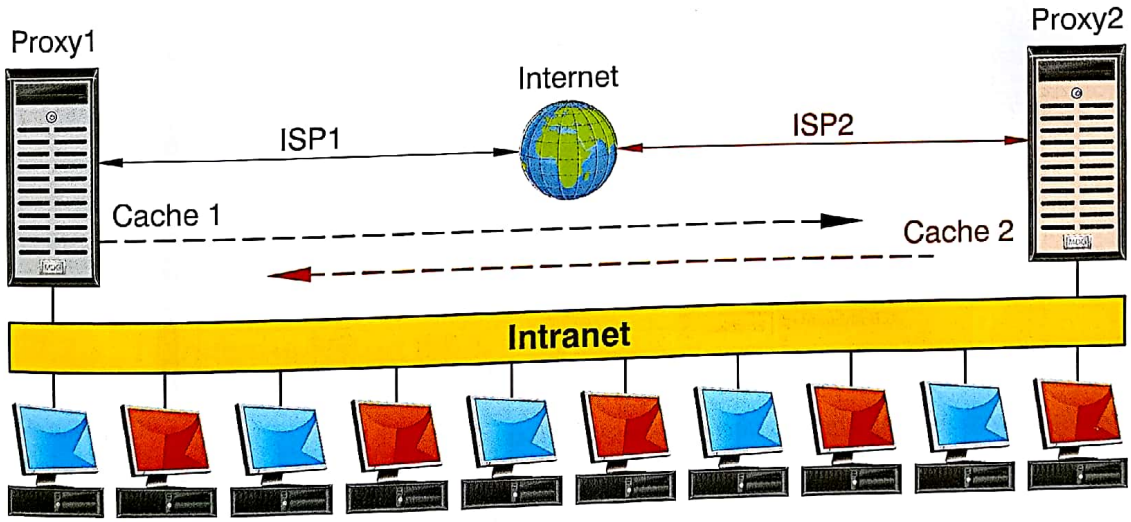

Bild 1.183: Zwei Proxies im Cacheverbund

Die Hälfte der Clients ist dazu konfiguriert, Proxy1 zu benutzen, die andere Hälfte benutzt Proxy2. Proxy1 verfügt über eine eigene physikalische WAN-Anbindung zu ISP1, Proxy2 über eine eigene physikalische WAN-Anbindung zu ISP2. Beide Proxies stehen zueinander in einem hierarchielosen Peer-to-Peer-Verhältnis (Sibling Relation) und arbeiten über Kreuz im Cache-Verbund. Das bedeutet, dass jeder Proxy bei einer Clientanfrage nach einer Ressource zuerst seinen Peer befragt. Nur wenn der Peer die Ressource nicht liefern kann, wird sie extern beschafft. Beide Proxies „teilen sich die Beute" – der externe Traffic jedes Proxies wird minimiert. Als Störfall wird nun definiert, dass durch Bauarbeiten, technische Probleme beim ISP oder Defekt eines Interfaces eine WAN-Anbindung ausfällt. Der betrof-

fene Proxy kann nun kurzfristig manuell dahin gehend **umkonfiguriert** werden, dass er seinen bisherigen Peer nun als hierarchisch höher stehend betrachtet *(Parent Relation)* und keine eigenen externen Beschaffungsversuche mehr unternimmt. Er befragt nur noch den (ungestörten) Parent. Die Clients bemerken dann nur die geringere Bandbreite.

Netzwerk-Management-Systeme

Netzwerk-Management-Systeme beruhen darauf, dass NICs, Hubs und Switches etc. mit sogenannter **Management-Agenten-Software** und ggf. (z. B. bei Hubs) auch mit Management-Agenten-Hardware ausgestattet werden. Die Management-Agenten registrieren vor Ort Ereignisse, sammeln sie und schicken Ergebnisse auf Anfrage zu einer **Management-Station**, auf der die eigentliche Management-Applikation läuft. Die Agenten können auch eigenständig Alarme auslösen. Die Management-Agenten kommunizieren mit der **Management-Applikation** meist über das zu administrierende Netz selbst *(„In-Band-Management")*. Dazu dient das UDP-basierte **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol).

Häufig sind in kleineren Netzen aber auch schon einfachere Lösungen verwendbar; so gibt es beispielsweise die Möglichkeit, einen Switch mit integriertem HTTP-Server über einen Browser zu verwalten (Bild 1.184).

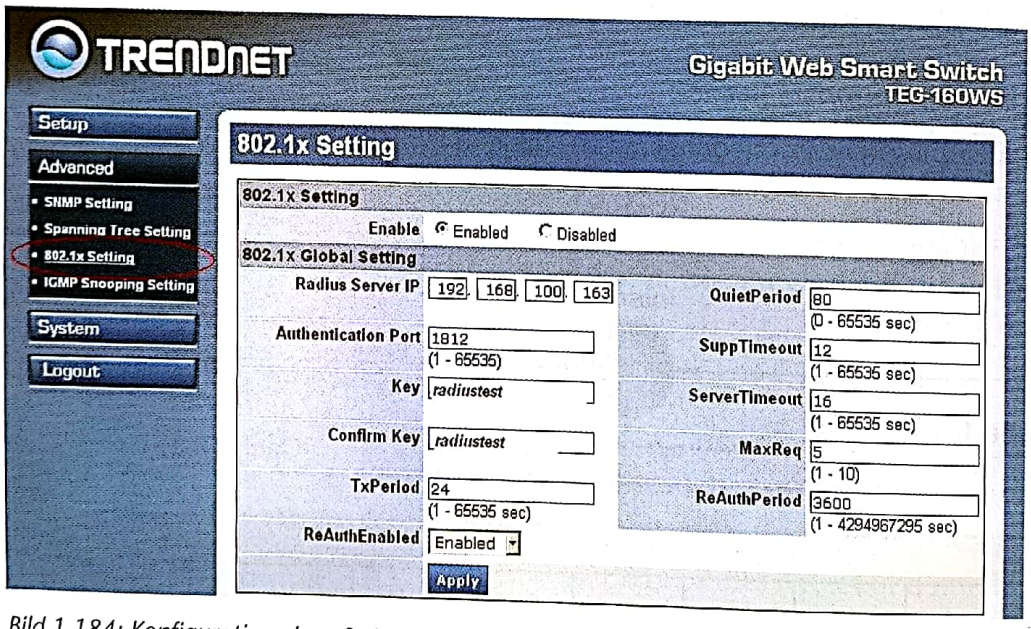

Bild 1.184: Konfiguration eines Switches über sein Web-Interface

Aufrechterhaltung der übrigen Informationssicherheit

Andere Begriffe hierfür sind auch **IT-Sicherheit**, **Datensicherheit** oder **Netzwerksicherheit** im Gegensatz zum **Datenschutz** (B 1.5).

Als Kurzfassung des BSI-Gefährdungskatalogs gilt es zu verhindern:

- Ausspähung von Daten durch nicht autorisierte Personen
- Veränderung gespeicherter oder übertragener Daten
- Fälschung von Identitätsdeklarationen

Diese Gefährdungen bestehen auch schon bei unvernetzten Computern und lassen sich durch geeignete Gegenmaßnahmen minimieren: Zwang zur Authentifizierung und Vergabe von Zugriffsrechten auf Betriebs- und Dateisystemebene (Kap. 2).

Organisatorische Maßnahmen:

1. Zugangskontrolle zu Server- und Verteilerräumen und gesondert den hierin befindlichen Schränken
2. Einweisung der Benutzer, z. B. in Passwortrichtlinien
3. Gewährung eines Benutzerkontos nur nach Quittierung einer Benutzerordnung
4. Gewährung des Netzzugangs nur nach vorheriger, passwortgesicherter Anmeldung

Technische Maßnahmen:

1. Einschränkung der technischen Möglichkeiten bei den Clients (z. B. unkontrolliertes Booten vom USB-Speicher)
2. Verteilung aller Netzdienste auf möglichst viele Servermaschinen, insbesondere eigene Nameserver
3. Abschalten nicht gebrauchter Serverprozesse auf jeder Servermaschine
4. Verzicht auf unsichere Dienste. Beispiel: Bei Telnet wird das Passwort im Klartext übertragen und kann insbesondere bei Verwendung von Hubs leicht ausgespäht werden ⇒ Ersatz von Telnet durch SSH (Secure Shell, Telnetersatz mit guter Verschlüsselung) und ggf. Ersatz von Hubs durch Switches
5. Einsatz spezieller Überwachungssoftware mit dem Ziel, unautorisierte (erfolgte) Eingriffe aufzuspüren (Intrusion Detection System)
6. Einsatz von Firewalls
7. Installation von Verschlüsselungssoftware auf Systemebene (VPN) und Anwendungsebene
8. Zentralisierte Authentifizierung

Ausführlichere und breiter angelegte Handlungsempfehlungen können wiederum dem BSI-Maßnahmenkatalog entnommen werden. Den Punkten 6 und 7 sind die nachfolgenden Unterkapitel gewidmet.

1.7.2.3 Technische Mittel der IT-Sicherheit

Firewall

Ausführlicher wird nun ein Baustein betrachtet, der in jeder Sicherheitskonzeption unerlässlich ist: die **Firewall** (engl. für Brandschutzmauer) – der Katalog spricht im Baustein B 3.301 allerdings von einem **Sicherheitsgateway**, um anzudeuten, dass die Schutzfunktion oft nicht mehr von nur einem Gerät, sondern von einer Reihe von IT-Systemen ausgeübt wird.[1]

Die Firewall soll eine Hürde zwischen zwei Netzen darstellen, die für Unberechtigte möglichst unüberwindlich ist. Sie ist meistens auf dem Router zwischen lokalem Netz und öffentlichem Weitverkehrsnetz angesiedelt (Bild 1.185). Für die Konstruktion einer Firewall stehen grundsätzlich zwei Elemente zur Verfügung: Proxies und Paketfilter.

[1] *IT-Grundschutz-Kataloge, 2011, S. 190 ff.*