Pit FRITZ, Eggweg 4, 8810 Horgen, email: pit@fritz.net

Überlegungen von P. Fritz zur

PC- und Netzwerk-Architektur der Schule Horgen

vom

24. März 2001

Zusammenfassung

Das vorliegende Konzept ist in drei Teile unterteilt.

- Im Teil *Motivation* wird beleuchtet, warum die Schule überhaupt ein Netzwerk braucht, und welche Software verwendet werden soll.
- Im Teil *MS-Windows 2000* wird ein Überblick über Windows 2000 und seine Möglichkeiten gegeben. Es werden einige Konzepte eingeführt, die dann in der effektiven Realisierung des Netzwerkes zur Anwendung gelangen. Gute Kenner von Windows 2000 können diesen Teil überspringen.
- Im *dritten Teil* wird dann konkret ausgeführt, wie die Hardware und Software konfiguriert werden soll.

Im Anhang wird auf das Prinzip und die Konfiguration des Virtual Private Network (VPN) eingegangen.

Inhalt

Motivation

In den Anfangszeiten der Netzwerke stand ein zentraler Grosscomputer (Mainframe) zur Verfügung, zu dem sich die dezentralen Clients via „dumme“ Terminals verbanden. Diese Mainframes waren teuer hinsichtlich Anschaffung und Wartung, und anfällig gegen Versagen, da sie einzig waren. Sie waren nicht skalierbar: bei grösseren Anforderungen musste der Mainframe ersetzt werden.

Die meisten dieser Probleme wurden mit der Einführung des Client/Server Prinzips gelöst, in dem mehrere Server zur Verfügung standen, und die Clients eine lokale Intelligenz erhielten. Der Preis dafür bestand in einem grösseren Overhead für die Administration, Problemen für den Benutzer die gewünschten Resourcen in einem verzweigten Netzwerk zu finden, und Problemen der Sicherheit, die mit Mainframes zentral viel einfacher hatten kontrolliert werden können.

Es ist nun die Aufgabe von Netzwerkbetriebssystemen, diese Probleme zu lösen, vornehmlich durch drei Massnahmen:

1. Logische, aber nicht physische Zentralisierung der Administration
2. Vereinheitlichtes Verzeichnis (directory) für alle Resourcen (objects), beispielsweise Benutzer, Benutzergruppen, Organizational Units, aber auch Dateien, Drucker usw.
3. Hierarchische Strukturierung des Netzwerkes.

Vor dem Eintauchen in Details soll aber erwähnt werden, warum eine Schule überhaupt ein Netzwerk braucht. Dabei muss unterschieden werden zwischen lokalen Netzwerken (local area networks (LAN)), z.B. in einem einzelnen Schulhaus, und einem Zusammenschluss dieser LANs zu einem logisch übergeordneten Netzwerk (der physische Zusammenschluss erfolgt ohne weitere Massnahmen via Internet).
Gründe für den Zusammenschluss in LANs:

- Internetanschluss (Begründung siehe Informatikkonzept der Primarschule Horgen, http://pit.fritz.net/schule).
- Datenaustausch.
- Benützung gemeinsamer Resourcen (z.B. Printer).
- Client/Server Vorteile.

Gründe für einen Zusammenschluss aller LANs zu einem Netzwerkverbund:

- Vereinfachung der Administration und des Unterhalts durch Zentralisierung und Vereinheitlichung (siehe Demo unter http://www.microsoft.com/windows2000/guide/autodemos/demos/mod02.htm).
- Reduktion Fachpersonal für dezentrale Administration.
- Einfache Zusammenstellung aller Resourcen des ganzen Schulnetzes zwecks Inventarisierung und zur Verfügung stellen.
- Remote Installation von SW auf Client PCs über das Netz, vollkommen transparent für den Client.
- Benützung gemeinsamer Resourcen über Klassenzimmer- und Schulhausgrenzen hinweg (z.B. Applikationen, farbiger A3-Laserprinter, DVD Brenner für Videos).
- Lizenz Management (von Software).
- Roaming Users über Klassenzimmer- und Schulhausgrenzen hinweg.

Gemäss Aussagen von Peter Suter, Leiter Weiterbildung Informatik am Pestalozzianum, werden die zukünftigen „Tipps für die Hardwarebeschaffung“ des Pestalozzianums eine Vernetzung als integrierenden Bestandteil jeder Beschaffung beinhalten.

Als Beispiel hierzu möge der Bericht von C. Smith dienen, der für seine Firma in 14 geographisch unabhängigen Orten 1600 Users zu betreuen hatte, und dafür an jedem Ort einen Systemadministrator brauchte. Seit dem logischen Zusammenschluss in ein einziges Netzwerk werden für die Administration insgesamt nur noch zwei Systemadministrator gebraucht (http://www.windows2000advantage.com/case_studies/11-06-00_grouppolicy.asp?s=9017).

Als Netzwerkbetriebssystem kommen nur zwei Plattformen in Frage:

- Unix bzw. Linux
- Microsoft Windows 2000.

Unix kann auf die längste Geschichte zurückblicken und ist daher bewährt und stabil. Es eignet sich v.a. für grosse und grösste Netzwerke, die von Experten administriert werden.
In seiner neuesten Inkarnation, der fünften, hat Microsoft (MS) mit **Windows 2000** ein Netzwerkbetriebssystem eingeführt, das theoretisch alle Anforderungen für einen Betrieb der Grösse der Schule Horgen erfüllt, und praktisch dank seiner Geschichte robust und erst noch einfach administrierbar ist. Dies dank seinem gleichen "Look- und Feel" wie dem Windows auf den Client PCs und dem durchgehenden grafischen User Interface. Im Gegensatz zu Unix kann sich ein Windows Power User relativ einfach in die Administration von Windows 2000 einarbeiten. Der grundlegende Design eines grösseren Netzwerkes braucht aber auch hier spezielles Fachwissen.
Gute anwendungsorientierte Kommentare zu Windows 2000 werden von der ETH zur Verfügung gestellt (http://www.windows2000.ethz.ch/Win2000info/Win2000info.htm).

Aus diesen Gründen stellt die Schule Horgen auf Windows 2000 als Netzwerkbetriebssystem ab. Dies hat auch noch den weiteren Vorteil, dass die vorhandenen PCs, die mehrheitlich ebenfalls unter Windows laufen, problemlos darin eingebunden werden können.
Gemäss Literatur können auch Macs daran anbinden. Wie einfach bzw. mit welchen Detailproblemen dabei gerechnet werden muss, ist dem Unterzeichnenden unbekannt.

Im folgenden soll gezeigt werden, wie MS die oben erwähnten drei Probleme jedes Netzwerkbetriebssystemen löst.

MS-Windows 2000

MS-Management Console (MMC)

MMC stellt einen zentralen Container dar als Interface zu allen Administrativen Tools eines Netzwerkes und zum Monitoring des Netzwerkes selbst. MMC ist erweiterbar, indem einzelne sog. Snapins zugefügt werden können zur Administration beliebiger Objekte. Solche Snapins gibt es für die Administration der Active Directory (AD), der Remote Access Services (RAS), Group Policies (GPOs), Internet Information Services (IIS), usw.

Active Directory

Im Jargon von MS heisst das vereinheitlichte Verzeichnis **Active Directory** (AD). Sie dient als zentraler Informationsspeicher der Netzwerkumgebung, dank ihrer Replikations Möglichkeiten aber in einer verteilten Form. Die Beschreibung ihrer möglichen Klassen von Resourcen wird in einem sog. Schema abgelegt, das auch Teil der AD ist.

Die einzelnen Resourcen der AD werden aufgrund ihrer **Domain Name System** (DNS) Namen gefunden, die auf Anfrage von DNS Servers in ihre IP Adresse übersetzt werden.
DNS ist notwendig um die AD zu konfigurieren. Ein DNS Server muss als Minimum folgendes unterstützen:

- Service Location (SRV) resource records: um einen Domain Controller zu finden wird ein DNS Server angefragt nach SRV resource records die dem AD Domain Name entsprechen. Dieser gibt dann den DNS Namen des Domain Controllers zurück.
- Dynamic Updates: PCs registrieren Records auf dem DNS Server dynamisch, z.B. kann einem Domain Namen nach jedem Einloggen eine andere IP Adresse zugeordnet werden. Bei der Suche nach dem Namen wird dann die aktuelle IP Adresse gefunden.

Die Namespaces von AD und DNS sind unabhängig und haben eine andere Struktur. AD basiert auf Domains und enthält Domain Objects. DNS enthält Zones (entsprechend domain names in AD) und Resource Records.

Üblicherweise wird zuerst der AD Namespace definiert, wo die Namen die Hierarchie der Domains und Subdomains wiederspiegeln (z.B. lehrer.bergli.schule.horgen.ch), welche dann auf dem DNS Server eingetragen werden. Es dürfen nie zwei gleiche Namen verwendet werden. Die Replikation übernimmt die AD, der DNS Server selbst muss nicht repliziert werden. Es können auch zwei DNS Server konfiguriert, einer nur für interne Namen, der andere nur für externe. Um Suchen zu vereinfachen kann der interne DNS Namespace von einem anderen Rootnamen ausgehen.

AD unterstützt mehrere Namensformate:

- Universal Naming Convention (UNC), z.B. \\mygroup.mycompany.ch\pathspec\filename.xls
- Hypertext Transfer Protocol (HTTP), z.B. http://mygroup.mycompany.ch/pathspec/filename.htm
- RFC 822 (Internet e-mail), z.B. myname@ mygroup.mycompany.ch

Strukturierung des Netzwerkes, oder Windows 2000 Domänen Konzept

Einleitung

Mit Windows 2000 werden die Begriffe Standort (Site), Organisationseinheit (OU), SDOU (Site, Domäne, Organisational Unit), Wald (Forest), Baum (Tree), Root-, Parent- und Child-Domäne, angrenzende (contiguous) und nicht-angrenzende (non-contiguous) Namen, transitive Kerberos-Trusts (gegenseitige, durchgehende Vertauensstellung innerhalb eines Waldes) - um einige zu nennen - im Zusammenhang mit der Domänen-Architektur eingeführt. Diese Begriffe sollen kurz erklärt werden.

Die erste installierte Windows 2000 Domäne, d.h. der erste installierte Domänenkontroller, eines Waldes bildet die Root-Domäne und konstituiert damit eine Site, eine Domäne und eine Organisationseinheit (SDOU) mit einem Schema und einem Global Catalog. Ausgehend von der Root-Domäne kann ein Baum mit Child-Domänen (contiguous Namen) oder weitere Bäume (non-contiguous Namen) erstellt werden. Der Wald ist eine Einheit, die mit dem Begriff 'Enterprise' zusammengefasst wird. Innerhalb des Waldes kann eine multi-level Hierarchie von Domänen und Organisationseinheiten konstruiert werden. Die Organisationseinheiten können User-, Gruppen, Computer-, Filefreigabe-, Drucker-, Kontakte- und weitere OU-Objekte enthalten. Die Delegation der Administration ist bis auf Attribut-Ebene innerhalb einer Organisationseinheit möglich.

Domains

The core unit of logical structure in AD is the domain. Grouping objects into one or more domains allows the network to reflect the company's organization**. A domain stores information about the objects it contains only.**
Bestehen innerhalb einer Domain mehrere Domain Controllers (DC) (z.B. zwecks Ausfallsicherheit), so wird die AD dieser Domain automatisch auf alle DCs repliziert. Soll die Replikation nur zw. einzelnen PCs oder zu gewissen Zeiten erfolgen, so müssen verschiedene Sites eingeführt werden.
NB: Eine Replikation der ADs zwischen verschiedenen Domains findet nicht statt.

A domain is a single security boundary of a Windows 2000 computer network. The AD is made up of one or more domains. A domain can span more than one physical location. Every domain has its own security policies and security relationships with other domains. A domain administrator has absolute rights only for his domain. Access to domain objects is controlled by access control lists (ACL). All security polices and settings – such as administrative rights, security policies and ACLs – do not cross from one domain to another.

Zwischen beliebigen Domains gilt unter Windows 2000 standardmässig ein Zweiweg-, transitiver Trust. Dies bedeutet, wenn Domain A der Domain B vertraut, dann gilt dies auch umgekehrt. Als Folge gilt aber auch, wenn Domain A der Domain B vertraut, und Domain B der Domain C, dann vertraut A auch C und umgekehrt.

Konsequenzen:
- Innerhalb einer Domain kann ich Permissions zu Objekten festlegen für User oder Gruppen von anderen Domains.
- Hat ein User eine Permission für ein bestimmtes Objekt einer Domain, so kann dieser User das Objekt von allen Domains aus benutzen.

Organizational Units

Die Organizational Units (OU) sind Container innerhalb einer Domain die eine Strukturierung der Objekte erlauben. Dies kann aus zwei Gründen geschehen:
- um die Organisationsstrukur besser wiederzugeben
- um die Administration an einzelne (kleinere) Units delegieren zu können.

Die Administration einer OU kann bis auf Attribut-Ebene delegiert werden. Da die Security Boundary durch die Domain und nicht durch die OU definiert wird, ist es einfacher Objekte innerhalb einer Domain zu verschieben als über Domain Grenzen hinweg. OU erlauben dies trotz der (teilweisen) administrativen Unabhängigkeit.

Domain Trees

A domain tree (a tree) is comprised of several domains that share a common schema and configuration, forming a contiguous namespace. Domains in a tree are also linked together by trust relationships. The AD is a set of one or more trees.

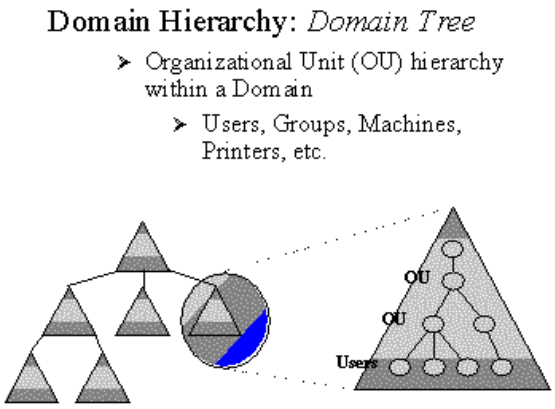

Fig. 1: Domain Tree

Trees can be viewed two ways. One view is the trust relationships between domains. The other view is the namespace of the domain tree.

A tree is defined by:
- A hierarchy of domains
- A contiguous namespace
- Transitive Kerberos trust relationships between the domains (consequences c.f. discussion of domain)
- A common schema
- A common global catalog (but each domain has it's own AD)

Trees unterstützen desweiteren die Vererbung von Group Policies. Group policies are cumulatively inherited down the tree hierarchy.

Forests

Multiple domain trees can be connected together into a forest.
A forest is defined by:

- One or more sets of trees
- Disjointed namespaces between these trees
- Transitive Kerberos trust relationships between the trees (consequences c.f. discussion of domain)
- A common schema
- A common global catalog

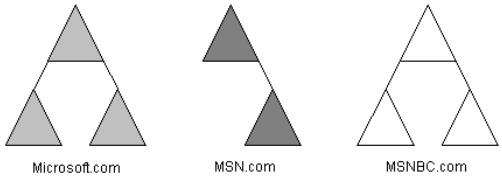

Fig. 2: Forest

Global Catalog

Um Informationen in der AD schnell auffinden zu können, und um den Network Logon zu ermöglichen, gibt es den Global Catalog. Dabei handelt es sich um einen einzigen Index über alle Domänenbäume in einem Wald (Forest) hinweg. Wird z.B. in einem Forest nach allen Printern gesucht, so erfolgt dies effizient via den Global Catalog. Ohne ihn müsste die AD jeder Domain einzeln abgefragt werden.
Es sollten immer mindestens zwei GCs pro Forest installiert werden (Redundanz) Wird ein Forest über verschiedene Subnets (oder gar Sites) betrieben, bringt ein GC pro Subnet (bzw. Site) einen Performance-Vorteil.

Im Schemamanager kann bestimmt werden, welche Objekte im Global Catalog indexiert werden sollen (Zum Beispiel Username, Druckername usw.). Standardmässig sind es alle Objekte aber mit je nur einer kleinen Anzahl von Attributen (die am öftesten gesuchten).

Sites

A site is a location in a network that contains AD servers. A site is defined as one or more well-connected TCP/IP subnets. "Well-connected" means that network connectivity is highly reliable and fast (for example, LAN speeds of 10 million bits per second or greater). Defining a site as a set of subnets allows administrators to quickly and easily configure the AD access and replication topology to take advantage of the physical network. When a user logs on, the AD client finds AD servers in the same site as the user. Because machines in the same site are close to each other in network terms, communication among machines is reliable, fast, and efficient. Determining the local site at logon time is accomplished easily because the user's workstation already knows what TCP/IP subnet it is on, and subnets translate directly to AD sites.

Eine Site ist nicht Teil der logischen Domain Hierarchie, sondern bildet eine unabhängige physische Hierarchie. Mittels Browsing werden beispielsweise nur Objekte (z.B. PCs) gefunden mit ihrer Zuordnung zu einer Domain oder OU, aber nicht zu einer Site.
Eine Site ist deshalb dann erforderlich, wenn Standorte einer einzigen Domain über langsame Netzverbindungen (<128 kbs) verbunden sind. Eine einzelne Domain kann sich über mehrere Sites erstrecken, und eine Site kann PCs enthalten die verschiedenen Domains angehören. Die

Replikation zwischen Domaincontrollers einer Domain innerhalb einer Site geschieht automatisch und ohne Kompression der Daten, jene zwischen Sites erfolgt komprimiert und kann zeitlich gesteuert werden.
Um die Performance Vorteile zu nützen soll jede Site mindestens einen AD Server und einen Global Catalog Server beinhalten. It seems not to be compulsory that each site has it's own DC (but recommendable), because a PC automatically looks for the next DC within it's domain.

A domain structure with 3 or more sites requires a centralized DHCP structure in which each site has it's own DHCP server.

Kommunikation innerhalb Netzwerk und zum Internet

Problemstellung

Die Kommunikation innerhalb eines Wide Area Networks (WAN), d.h. zwischen örtlich verteilten LANs, ist auf verschiedene Arten möglich. Der Spezialfall bei der Schule Horgen besteht darin, dass diese Kommunikation möglichst günstig bewerkstelligt werden soll. Da die zu verbindenden Schulhäuser mehrere Kilometer auseinanderliegen, drängt sich deshalb als Transportmedium das Internet auf. Jeder PC im Internet muss eindeutig adressierbar sein. Die Miete solcher Adressenbereiche (Internet Protocol (IP) Nummern) ist aber teuer, deshalb soll pro Schulhaus nur eine einzige IP-Nummer gemietet werden. Alle anderen PCs in jedem Schulhaus-LAN haben sog. private IP-Nummern: diese sind gratis, dafür aber nicht zulässig im öffentlichen Internet.
Folgende IP-Nummern sind privat:

Network Class	Network Prefix	Host Nummern	IP Nummern	Network Mask	Subnet Mask	Anzahl Sub-netze	Anzahl Hosts/ Netz
A	8 bit:	3x8=24 bit	10.0.0.0 bis 10.255.255.255		255.0.0.0	1	256^3
B	16 bit:	2x8=16 bit	172.16.0.0 bis 172.31.255.255	255.240.0.0	255.255.0.0	16	256^2
C	24 bit	8 bit	192.168.0.0 bis 192.168.255.255	255.255.0.0	255.255.255.0	256	256

Die Verbindung von LANs mit privaten IP-Nummern zu einer einzigen Windows 2000 Domain ist speziell und bedarf verschiedener Abklärungen.

Network Address Translation und Internet Connection Sharing

Network Address Translation (NAT) is one possibility to connect a LAN to the Internet through a single Internet connection and a single IP address.
NAT ersetzt die private IP-Nummer des anfragenden PCs durch eine öffentliche IP-Nummer (diejenige des NAT-Servers) und eine Port-Nummer. Die Antwort des angefragten Servers enthält dann diese Port-Nummer, womit die ANtwort an die korrekte (private) IP-Adresse weitergeleitet werden kann.

Advantages:
- With NAT one can use unregistered IP addresses for the internal LAN.
- simple configuration.

Disadvantages:
- NAT does not support Kerberos and Internet Protocol Security (IPSec). Therefore a secure authentification is not possible directly from a NAT router.
- MS recommends (c.f. Q254018) never to use the Point-to-Point Tunneling Protocol (PPTP) from a NAT router because due to the unsafe connection. One would open security holes to the corporate network. However, from a PC in the NAT LAN it's possible to establish a PPTP (c.f. Chap. 22, pp. 816 of the Windows 2000 Server Resource Kit Deployment Planning Guide).
- Logging on to a domain from a NAT LAN with Windows < 2000 is not possible, because NETLOGON does not work over an unsafe connection. To log on one needs to first creating a Virtual Private Network (VPN) connection over Routing and Remote Access Services (RRAS). Logging on to a domain from a NAT LAN with Windows 2000 is possible, because Windows 2000 does not log on by NETLOGON, but rather by locating a DC.

Therefore a NAT router cannot be integrated into the AD hierarchy of a corporate network. However it could be used to directly connect to the Internet. For details see http://www.microsoft.com/TechNet/cableguy/cg0301.asp .

Internet Connection Sharing (ICS) is similar to NAT, easier to configure, but limited to a single subnet and a single connection to the Internet.

Routing and Remote Access (RRAS)

Routers forward data from one subnet to another (or from one type of network to another, e.g. from ETHERNET to ATM (Asynchronous Transfer Mode)). Windows 2000 supplies routing from LAN to LAN without the need of special Hardware.
RAS provides remote office connectivity by supporting dialup connections via the Point-to-Point Protocol (PPP). PPP supports authentication, but no encryption.
RRAS provides remote office connectivity by supporting WAN connections (via dialup or VPN).

WAN connections may be established based on PPTP or the Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec). PPTP supports user authentication and encryption, and routes IP and IPX/SPX traffic. P2TP/ IPSec supports user and data authentication, encryption and data integrity, but routes IP traffic only. L2TP/IPSec provides more security then PPTP, but requires to apply for and exchange certificates between clients and servers before connecting.

Clients access the corporate LAN through a VPN over a RRAS server. RRAS allows several ways to to maximize speed and security.

Virtual Private Networking (VPN)

A virtual private network (VPN) is the extension of a separate network that encompasses links across shared or public networks like the Internet. To emulate a point-to-point link, data is *encapsulated*, or wrapped, with a header that provides routing information allowing it to traverse the shared or public internetwork to reach its endpoint (via PPTP or L2TP/IPSec). To emulate a private link, the data being sent is *encrypted* for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. VPN connections also allow organizations to have routed connections with geographically separate offices or with other organizations over a public internetwork such as the Internet while maintaining secure communications. A routed VPN connection across the Internet logically operates as a dedicated WAN link.
A router-to-router VPN connection is made by a router and connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server is attached. On a router-to-router VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers.

Usually the main office is pemanently connected to the Internet. However it is also possible to have both offices (remote and main) connected to the Internet using a demand dial-up WAN link. However, this is only feasible if the ISP supports demand-dial routing to customers; the ISP calls the customer router when an IP datagram is to be delivered to the customer.

Proxy and VPN Server

In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.
A proxy server receives a request for an Internet service (such as a Web page request) from a user. If it passes filtering requirements, the proxy server, assuming it is also a cache server, looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.
However a proxy server does not just support HTTP, but a multitude of other protocols, as , FTP, SMTP e-mail, H.323 conferencing, streaming media (MS Windows Media Technologies, RealAudio/RealVideo), remote procedure calls (RPCs), and more.

Da Proxy Server vielfach der einzige Schnittpunkt zum Internet sind, werden mit Proxy Funktionen oft auch Firewall Funktionen kombiniert. Der Nachfolger von MS's altbewährtem Proxy Server, der Internet Security and Acceleration (ISA) Server (Standard Edition $ 1'500.-/Server), unterstützt beispielsweise auch

- integriertes VPN,
- SecureNAT,
- Firewall Funktionen,
- Windows 2000 integriertes Management,
- mehr Filter (z.B. H.323 Filter and MS NetMeeting Gatekeeper),

- Hierarchisches Caching.

ISA Server extends the Windows 2000 network address translation (NAT) functionality by enforcing ISA Server policy for SecureNAT clients. In other words, all ISA Server rules can be applied to SecureNAT clients, despite the fact that Windows 2000 NAT does not have an inherent authentication mechanism. (Policies regarding protocol usage, destination, and content type are also applied to SecureNAT clients.)

Organisation

Group Policies

Group Policies (GPO) erlauben die Konfiguration von Desktop Environments über das ganze Netzwerk. Beispielsweise kann für eine bestimmte OU das Ausführen eines Logonscripts verlangt werden. Folgende Eigenschaften können mit GPOs vorgeschrieben werden:

- Computer Settings (z.B. Windows Settings, Network Bindings)
- User Settings (z.B. logon Scripts, Desktop Konfiguration)
- Registry Settings (z.B. für Applikationen)
- Folder Redirection (z.B. kann C:\EigeneDateien auf einem Server alloziert werden)
- Internet Explorer Settings
- Remote Installation Services und SW Installation für Computers oder Users
- Scripts (logon/logoff, startup/shutdown)
- Security Settings

Wie erwähnt unterstützen Domain Trees standardmässig die Vererbung von GPOs. GPOs werden kumulativ ab Definitions-Domain die Tree Hierarchy hinunter vererbt (ausser dies werde explizit unterdrückt).
GPOs können auch für eine Site definiert werden. Obwohl die Definition in einer bestimmten Domain (der Site) gemacht wird, gelten sie für alle Domains der Site !

Ein wichtiges Gebiet, das durch GPOs abgedeckt wird, ist die SW Installation und ihr Unterhalt.

Windows Installer / SW Installation and Maintenance Technology

Windows Installer unterstützt

1. Installation von Applikationen aufgrund von SW Packages
2. Vergebende (resilient) Installationen: falls ein kritisches File einer Applikation überschrieben wird, wird es automatisch aufgrund des SW Package wieder hergestellt ("Selbstheilung").
3. Komplette Deinstallation

Die SW Packages werden vom SW Hersteller in Form von .MSI-Files geliefert. Diese können durch .MST-Files modifiziert werden, z.B. Einbindung eines schweizerdeutschen Diccionaires. Es können auch eigene Packages (.ZAP-Files) kreiert werden, jedoch mit Einschränkungen: Kein Assignment, nur Publishing, keine vergebende Installationen.

Die SW Installation and Maintenance Technology beruht auf GPOs und ADs. In den GPOs wird eingetragen, für wen und wie eine Applikation zur Verfügung gestellt wird:
Assignment einer Applikation bedeutet, dass sie als Icon im StartMenu oder auf dem Desktop erscheinen, und dass die notwendigen Registry Änderungen durchgeführt wurden. Sie wurde aber noch nicht installiert. Erfolgt das Assignment für einen User, so erfolgt die effektive Installation bei erstmaligem Doppelklicken des Icons oder eines assoziierten Files.
Erfolgt das Assignment für einen Computer, so erfolgt die effektive Installation beim Booten des PC‘s.

Beim **Publishing** einer Applikation erscheint kein Icon, sondern nur ein Eintrag unter Add/Remove Programs (Registry Änderungen werden aber auch durchgeführt). Die effektive Installation erfolgt via Add/Remove Programs oder bei erstmaligem Doppelklicken eines assoziierten Files. Publishing kann nur für Users erfolgen, aber nicht für Computer.

Remote OS Installation Feature, a result of SW Installation and Maintenance Technology:
If the computer requests a service boot during its startup sequence (typically, through a specific function key during startup), the computer establishes a network connection and makes a request for any nearby Windows 2000 Server to host the service boot request. Then, the user is requested to log on and the Windows 2000 Remote Installation Services then uses Group Policy to identify what configuration of Windows 2000 Professional the user is assumed to install. and the system automatically loads the appropriate configured version of Windows 2000 Professional.

Disks und Files

Basic Disks
Es gibt zwei Arten von Disks: Basic Disks und Dynamic Disks.
Basic Disks (default): müssen in maximal 4 Partitionen unterteilt werden:
Primary Partition (max. 4): Jede prim. Partition wird formatiert und erhält einen Laufwerksbuchstaben. Eine davon wird als aktiv bezeichnet, von der gebootet wird (= System Partition). Es scheint, dass die aktive Partition immer den Buchstaben C: erhält.
Extended Partition (max.1): Wird in eine oder mehrere Laufwerke (=Volumes) unterteilt, die je einen Laufwerksbuchstaben erhalten und formatiert werden. Removable Disks können keine Extended Partitions enthalten.
System Partition (immer C:): Aktive Partition, welche die Hardware spezifischen Files enthält.
Boot Partition: Primary oder extended Partition, welche das Betriebssystem enthält.

Dynamic Disks
Dynamic Disks enthalten eine einzige Partition, die in eine unbeschränkte Anzahl Volumes unterteilt werden kann. Ein Simple Volume beschränkt sich auf einen dynamic Disk, ein Spanned Volume verteilt sich auf mehrere.

Portable PCs können keine Dynamic Disks enthalten.
Die System Partition kann nie auf einer Dynamic Disk sein, sie ist immer die aktive primary Partition.

Die Boot Partition kann nicht auf einer neu kreierten Dynamic Disk sein, da eine solche keine Partition Table enthält. Allerdings kann sie zuerst auf einer Basic Disk eingerichtet werden, welche darauf zu einer Dynamic Disc promotet wird. Dabei wird jede Partiton in ein Volume umgewandelt. Die Grösse des Boot Volumes kann anschliessend nicht mehr verändert werden (sagt MS).

Filesyteme
Die Speicherung und Verwendung der lokalen Daten wird durch das sog. Filesystem gewährleistet, unter Windows 2000 üblicherweise dem NT-File Sytem (NTFS).

Ein Distributed File System (DFS) ermöglicht den Zugriff auf Daten die auf remote Servern residieren. Das DFS von Windows 2000 ist ein logisches, hierarchisches Filesystem, welches auf mehreren Servern verteilte Folders oder auch andere DFS Strukturen in einer einzigen Folderstruktur abbildet. Wird die Topologie lokal in der Registry abgelegt, so spricht man von einem standalone DFS, residiert sie in der AD heisst spricht man von einem Domain, Directory Enabled oder auch Fault-Tolerant DFS.
"Fault-Tolerant" bezieht sich sowohl auf die Speicherung der Struktur selbst, als auch auf die Daten, da Child Nodes der DFS auf mehrere identisch gesharte Folders zeigen können (sog. Alternate Volumes). Dem Client wird dann randommässig eines dieser Volumes zugeordnet, das auch effektiv online ist. Üblicherweise beinhalten die Alternate Volumes synchronisierte bzw. replizierte Daten.
Der Root Node einer DFS Struktur kann unter Windows 2000 nur auf einem Server (d.h. nicht auf einer Workstation mit Windows Professional) definiert werden, but any share or volume accessible through the network can participate in the Dfs name space (Begrenzung: Windows Workstations erlauben nur 10 Clients gleichzeitig).

Ein File auf einem Netzwerk kann durch seinen Universal Naming Convention (UNC) Namen aufgerufen werden, in der Form

\\Server\Share\Path\Filename.

Als Server kann auch der lokale PC-Name eingesetzt werden (Achtung: ein PC Name darf höchstens 15 Zeichen beinhalten, wobei nur Buchstaben, Zahlen und "-" zugelassen sind).
Auch wenn UNC Namen direkt verwendet werden können, werden sie typischerweise auf einen Laufwerksbuchstaben gemapt, d.h. x: weist auf \\Server\Share.
Ein File einer DFS Struktur kann ebenfalls durch seinen (virtuellen) UNC Namen aufgerufen werden, in der Form

\\Server\DfsShareName\Path\File

where Server is the name of the host DFS computer name, DfsShareName maps to any share that is designated to be the root of the DFS. One can net use a drive to any place in the DFS.
Bei Domain DFSs erhält die DFS einen Namen der in der AD gespeichert wird. Solche DFSs können dann auch zusätzlich durch

\\DoaminName\DFSName\Path\File

oder

\\DFSName\Path\File

aufgerufen werden.

Der Vorteil eines DFS besteht darin, dass die für den Benützer ersichtliche logische Struktur unabhängig von der physikalischen ist (dem Ort, wo die Daten auch wirklich gespeichert sind). Dies erleichtert sowohl dem Benützer das Auffinden von Files, als auch dem Admini-

strator die Verwaltung, da Folders verschoben werden können ohne Information des Benützers, nur die DFS Struktur muss angepasst werden.

Aufruf von Programmen
Wie beim DFS gezeigt ist es sehr nützlich, wenn der phsysikalische Ort, an dem ein Programm gespeichert ist, für den Benützer möglichst transparent ist. Fällt ein Server aus, so kann das Programm von einem anderen Server geladen werden. Dies wird durch das Konzept des DSF unterstützt. Ein anderes, fast wichtigeres Beispiel wäre das Versagen des ganzen Netzwerks. Dies muss nicht unbedingt ein Versagen sein, sondern kann auch gewollt passieren, wenn z.B. ein Notebook vom Netz abgehängt wird um unterwegs oder zu Hause zu arbeiten. In diesem Fall hilft ein DFS leider nicht mehr, da der Root Node desselben auf einem Server sein muss, und auf einem Notebook nur die Workstation Version von Windows installiert sein wird.
Im folgenden wird ein Konzept vorgestellt, welches diesen Anforderungen gerecht wird.

Wo ein Programm residiert ist in der Registry gespeichert, wobei pro Programm sehr viele Einträge vorhanden sein können. Um Probleme zu vermeiden gehen wir vom Grundsatz aus, dass die Registry nicht geändert werden soll, auch wenn das von variablen Orten geladen werden soll.
Da der Link in der Registry demzufolge konstant bleibt, muss das Ziel des Links angepasst werden. Dies erfolgt am einfachsten dadurch, dass in der Registry ein Alias verwendet wird, dessen Inhalt vor dem Programmaufruf angepasst wird.
Ein Programm Aufruf in der Registry kann entweder via Laufwerksbuchstaben, oder mit dem UNC Namen erfolgen. Desweiteren können in der Registry auch Environment Variablen verwendet werden. Allerdings muss der Datentyp des Eintrags als REG_EXPAND_SZ definiert sein. In Erweiterung des String-Typs REG_SZ expandiert dieser Typ Environment Variablen.

Beispiel 1: In der Registry steht ein Eintrag mit einem Laufwerksbuchstaben:
@="j:\\program files\\pshop.exe"
Es gibt mehrere Möglichkeiten, den Inhalt anzupassen:
1. j: wird mit NET USE auf einen anderen Folder umgeleitet.
   Vorteil: einfach
   Nachteil: kann nur einmal (z.B. beim Booten) gemacht werden, da sonst Inkompatibilitäten mit schon laufenden Programmen entstehen können. D.h. eine Zuordnung kann nicht pro Programm erfolgen, sondern nur pro Bootsession, und gilt dann für alle Programme auf j: (granular (d.h. aufteilbar) für jeden PC individuell bis auf Driveniveau).
2. Jeder Registry Eintrag, der ein Programm aufruft, wird ersetzt durch den Aufruf eines Scripts, welches den Programmnamen als Parameter erhält, und das Programm aufruft, wobei der Ort mit Environment Variablen dynamisch angepasst werden kann.
   Vorteil: varierbar innerhalb einer Session, granular für jeden PC individuell bis auf Programmniveau.
   Nachteil: umständlich. Funktioniert nur bei direkten Programmaufrufen, aber nicht wenn der Programmname in der Registry als Parameter übergeben wird (selten!). Kann ebenfalls zu Inkomptaibilitäten mit schon laufenden Programmen führen, falls diese mehrmals auf die Registry zugreifen (selten!). Die Programmtypen (.exe, dll, ocx usw.) sind zu unterscheiden und entsprechend zu laden).
3. j: zeigt auf eine DFS Struktur auf einem Server (diese Struktur kann nicht auf dem lokalen PC residieren, da der PC üblicherweise als Workstation und nicht als Server konfiguriert

ist). Die Zuordnung sollte nur einmal erfolgen (z.B. beim Booten mit NET USE), da sonst Inkompatibilitäten mit schon laufenden Programmen entstehen können. D.h. eine Zuordnung erfolgt pro Bootsession, für alle PCs eines LANs.
Die DFS Struktur kann dynamisch durch den LAN Administrator oder mit einem Script und der Utility DfsCMD.exe auch während einer Session angepasst werden.
Vorteil: transparente, variable Programmallozierung, Ausnützung der Vorteile des DFS. Granular für die Gruppe aller PCs eines LANs bis auf Programmniveau.
Nachteil: funktioniert nur mit Netzverbindung, und wenn der Server mit dem DFS root node erreichbar ist. Also beispielsweise nicht für vom Netzwerk abgehängte Notebooks.

4. Kombination von 1 und 3: Es wird getestet, ob der PC am Netz ist. Wenn ja gelte 3, sonst 1.
   Vorteil: funktioniert für Betrieb mit und ohne Netzwerkanschluss.
   Nachteil: verschiedene Granularität.

Beispiel 2: In der Registry steht ein Eintrag mit einem UNC Namen:
@="\\server\\program files\\pshop.exe"
"server" kann nicht umgeleitet werden.

5. Vorteil: keinen.
   Nachteil: weniger flexibel als mit Laufwerksbuchstabe.

Beispiel 3: In der Registry steht ein Eintrag mit einer Environment Variablen:
@="%LOC%\\program files\\pshop.exe"
Die Variable LOC kann jederzeit sehr einfach verändert werden, für jeden PC individuell.

6. Vorteil: analog 1 bis 5, mit dem Vorteil, dass die Variable grundsätzlich jederzeit verändert werden darf, da der Drive (Server) von bereits laufenden Programmen nicht ändert. Gegenüber 3 Granularität für jeden PC individuell.
   Nachteil: keinen.

Alloziierung von Programmen
Distributed File Systems werden verwendet um die physikalische Allozierung von Files durch eine logische zu ersetzen. Üblicherweise wird auf eine DFS (dank AD redundant vorhandene und damit Fehler tolerante) Struktur zugegriffen, welche Links auf verschiedenste Server enthält.
Beim Netzwerk der Schule Horgen soll aber jede Site weitgehend selbständig sein, d.h. alle gebrauchten Programme werden auf dem in jeder Site vorhandenen Domain Controller gespeichert. Falls ein DFS zur Anwendung gelangen soll, muss dieses deshalb für jeden Site individuell sein, mit Links die meist nur auf Shares innerhalb der Site zeigen. Es muss deshalb auf jedem Domain Controller ein Standalone DFSs kreiert werden, das sich nur darin unterscheidet, dass die Mappings auf den lokalen Servernamen zeigen.

Im Normalbetrieb, d.h. bei Netzanschluss, sind bezüglich der Programmallozierung drei Fälle zu unterscheiden:

1. Programm ist immer auf einem Netzwerk-PC (üblicherweise dem DC).
   Vorteil: einfacher Unterhalt, Schonung der begrenzten Diskkapazitäten von Clients.
2. Programm ist immer auf dem lokalen Volume E: .
   Vorteil: schnellere Ladezeit, funktioniert auch bei Serverausfall.
3. Programm ist entweder lokal oder auf einem Netzwerk-PC. Einzelne Clients mit grösseren Diskkapazitäten könnten mehr ladezeitkritische oder wichtige Programme lokal vorhalten.

Was hat dies auf die Registryeinträge von Pfaden und Programmenu Items unter dem Startmenu für Konsequenzen? Fall 1 und 2 ist unproblematisch, da der Link konstant ist. Fall 1 kann ein DFS be- und dessen Vorteile ausnützen. Fall 2 zeigt wird ganz konventionell gehandhabt.
Fall 3 bedarf näherer Betrachtung. Im einfachsten Fall (3a) wird im vornherein eine Gruppe von Programmen identifiziert, die der Gruppe 3 angehören sollen, und alle immer pro PC lokal oder remote gespeichert sind. Diese Programme werden dann beim Booten der Gruppe 1 oder 2 zugeordnet.
Schwieriger ist der Fall (3b), wenn einzelne Programme dieser Gruppe lokal, andere remote gespeichert werden sollen, für jeden PC individuell. Zum Laden eines Programm werden die Informationen, von wo es geladen werden soll, entweder aus der Registry (z.B. infolge Doppelklicken auf einem Worddokument) gelesen, oder aus den Properties des Programmenu Items, falls das Programm durch Wahl eines Items unter dem Startmenu geladen wird.
Im ersten Fall muss vor dem Aufruf der Speicherort bekannt sein. Dies könnte erfolgen, indem der Benützer vorher ein Script ausführen muss, welches den Ort zuordnet. Solche Eingriffe sind aber für einen Schulbetrieb nicht zu empfehlen.
Im zweiten Fall, in dem der Benützer ein spezifisches Programmitem wählt, könnte ein Script geladen werden, das prüfen kann, wo das Programm residiert, und es dann entsprechend lädt. Ob sich diese Komplikation lohnt hängt vom Bedürfnis der Benützer ab.

IntelliMirror

IntelliMirror uses features in both Windows 2000 Server and Windows 2000 Professional to allow users' data, software, and settings to follow them. Essentially, IntelliMirror provides users with follow-me functionality for their personal computing environment. Users have constant access to all of their information and software, whether or not they are connected to the network. This includes:

- **User data**: the files, documents, spreadsheets, workbooks, and other information that users create and use to perform their jobs.
- **Software** installation and maintenance: the installation, configuration, repair, and removal of applications, service packs, and software upgrades.
- **User settings**: the customizations of operating system and applications which define the computing environment of a user, for example, language settings, custom dictionaries, desktop layout, color schemes, and other user preferences.

While **online**, IntelliMirror for roaming users is implemented by the possibility of Policies (see above) and and by storing the data in specified network locations while making it appear local to the user.
When **offline**, IntelliMirror is realized by the concept of **offline folders**: a network location is set to be available for offline use. When a user then saves a file to the folder, the save is performed to the network and synchronized back to the local computer. This synchronization occurs in the background, transparently to the user. The user works in the same way, whether on or offline, and is unaffected by temporary network outages. When a user works offline, either through choice, or because of a network failure, all modifications and changes to any user data are made to the local copy. Eventually, when the computer is reconnected to the network, resynchronization with the network copy occurs automatically. If the network copy and the local copy have both changed, the synchronization manager prompts the user as to whether to save both copies or to synchronize against one or the other.

Use offline folder settings on the server share where the user's info is stored
This is especially important for users with laptops. **Redirected folders** of any type should be coupled with offline files. The recommended configuration for offline files to use is:

• MyDocs:	Autocaching for Documents or Manual Caching for documents (if you want users to have to "pin" files)
• AppData:	Autocaching for Application Data of Programs
• Desktop:	Autocaching for Programs if the desktop is read-only
• StartMenu:	Autocaching for Programs

NB: The common dialogs have been updated in Windows 2000 to point to MyDocuments by default, encouraging users to save documents there. With Windows 2000-based networks, administrators can limit users to saving in their profile folders only, which enforces My-Documents as the Save location.

For more info see User Data and User Settings Step-by-Step Guide (http://www.microsoft.com/TechNet/win2000/userdata.asp#d).

Design und Organisation des Netzwerks der Schule Horgen

Strukturierung

Logische Strukturierung

Der schon weiter oben zitierte C. Smith ordnete alle 1'600 User einer einzigen Domain zu, welche entsprechend ihrer geographischen Region auf der zweiten Strukturierungsebene in 14 Organizational Units unterteilt wurde, wobei jede OU wiederum in weitere OUs unterteilt wurde, für jedes Geschäft in der Region.

Diese Struktur kann im wesentlichen auf die Schule Horgen übertragen werden. Einzelne Schuleinheiten haben kaum einen Bedarf an abgegrenzten, individuellen Sicherheitssystemen in Bezug auf Administrationsorganisation, Sicherheitspolicies usw. Deshalb soll das ganze Schulnetz durch eine einzige Domain gebildet werden.

Eine logische Strukturierung wird durch OUs erreicht: Für jede Schuleinheit wird eine eigene OU erstellt. Zusätzlich kann eine Organisations OU erstellt werden, in die z.B. die Verwaltung und die Schulpflege eingebunden werden kann.

Physische Strukturierung

In Horgen

Durch die denzentrale Lage der Schuleinheiten mit verschiedenen, z.T. langsamen Anbindungen ans Internet wird jedes Schulhaus als eine eigene Site generiert. Jede Site soll mindestens einen AD Server (Domain Controller) und einen Global Catalog Server beinhalten.

Im Schulhaus

Innerhalb jedes Schulhauses sieht die Netzstruktur prinzipiell gemäss Fig. 3 aus. Zu den einzelnen Komponenten ist folgendes zu bemerken:

Internet: Der Anschluss ans Internet erfolgt grundsätzlich in einer Weise, dass die Verbindung immer on ist und genügend Bandbreite zur Verfügung steht. Zur Zeit (März 2001) ist das nur via Kabel möglich (vgl. Offerte Cablecom Anhang 2). Demnächst sollte dies aber auch via xDSL (Swisscom) und der Initiative „Schulen ans Netz“ möglich sein, wobei die letztere Möglichkeit ev, günstiger käme (siehe http://www.ppp-sin.ch).

Zur Zeit ist das Schulhaus Arn noch nicht an Cablecom angeschlossen. Die Nachbarhäuser sind aber verkabelt.
Beim Schulhaus Horgenberg besteht keine Möglichkeit zum Anschluss an Cablecom. Entweder fährt man weiter mit ISDN (keine statische IP-Nummer, nicht immer verbunden!), oder am wartet auf xDSL.
Das Schulhaus, welches als zentraler Server Standort dient (z.B. Bergli), sollte für die VPN Verbindungen und als Webseitenlieferant mit einer grösseren Bandbreite und mehreren IP-Nummern angeschlossen werden (z.B. Webcom Standard), für die anderen genügt eine kleinere Bandbreite und eine statische IP-Nummer (z.B. Webcom Light).

Switch/Hub: Je nach Schulhausgrösse kann hier ein Hub eingesetzt werden statt einem Switch.

Stockwerk Hubs: Je nach Schulhausgrösse sollen die Stockwerk Hubs einzeln oder sequentiell an den Schulhaus Switch/Hub angeschlossen werden.
Klassenzimmer Hubs: Hierfür sind mind. 8-Port Hubs vorzusehen. Sie können je nach Anzahl Zimmer einzeln oder sequentiell mit dem Stockwerk Hub verbunden sein.

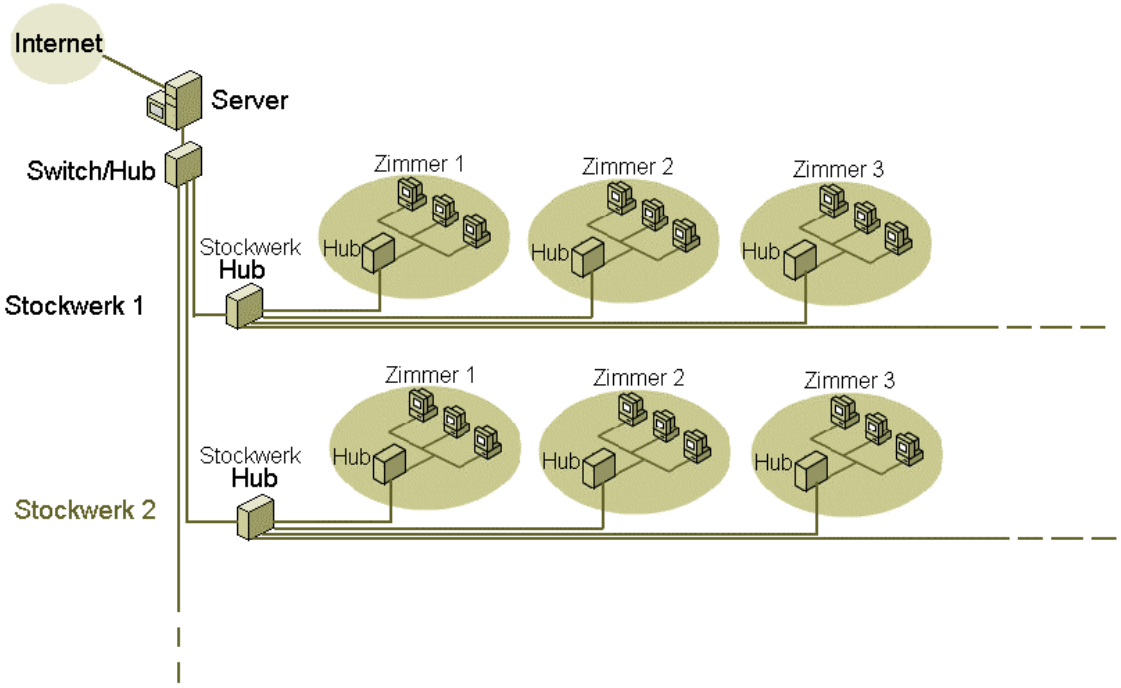

Fig. 3: Netzarchitektur innerhalb eines Schulhauses

Kommunikation

Anbindung einer Site ans Internet
Dies erfolgt via ISDN oder Kabel, in Zukunft ev. auch via xDSL (Digital Subscriber Line). Um den Zugriff auch von aussen zu erleichtern soll der Internet Service Provider (ISP) möglichst mind. eine statische, öffentliche IP-Nummer zuordnen. Falls dies nicht möglich ist (z.B. kein Kabelanschluss auf dem Horgenberg), erfolgt einseitiges Demand-Dialing via ISDN. Innerhalb der Site erhält jeder PC von einem DHCP-Server eine private IP-Nummer der Klasse B:

Network Class	Network Prefix	Host Nummern	IP Nummern	Network Mask	Subnet Mask	Anzahl Sub-netze	Anzahl Hosts/ Netz
B	16 bit:	2x8=16 bit	172.16.0.0 bis 172.31.255.255	255.240.0.0	255.255.0.0	16	256^2

Damit kann jeder Schuleinheit ein eigenes Subnetz zugeordnet werden. Für jedes Subnetz bzw. jede Schuleinheit stehen 256^2 = 65'536 IP-Nummern zur Verfügung (vgl. Anhang).

Verbindung zur Hauptdomain und zum Internet
In jeder Site wird ein Internet Security and Acceleration (ISA) Server eingerichtet, der eine VPN Verbindung zu und von allen anderen Sites gewährleistet.

Auf jedem ISA Server wird eine Local Address Tabel (LAT) definiert, mit allen IP Adressen die lokal sind oder die zu einer anderen Site gehören. Wird ein Request gemacht zu einer IP Nummer einer anderen Site, werden die Daten via VPN geroutet. Ist die IP Adresse nicht in der LAT enthalten, bedeutet dies ein Request zu einer Resource irgendwo auf dem Internet, der dann via SecureNAT an den Internet Service Provider (ISP) geleitet wird.
Details zur Wirkungsweise und Konfiguration von VPN für die Schule Horgen sind im Anhang enthalten.

Ein VPN Server muss in Bezug auf Schnelligkeit nur die minimalsten HW-Anforderungen erfüllen. Dafür sind Sicherheitsvorkehrungen Beachtung zu schenken, da er als einzige Maschine mit einer öffentlichen IP-Nummer direkt vom Internet her erreichbar ist. Minimalste Sicherheitsvorkehrungen sind folgende:

- ISA Server als Standalone Server aufzusetzen, also nicht als Domain Controller, und ihn nicht als Member einer AD Domain definieren.
- Nur die unbedingt notwendigen Accounts definieren (für Administration und VPN Clients).
- Keine nicht unbedingt notwendigen Services laufen lassen, wie z.B. Exchange, SQL, IIS, Proxy Server.
- MS empfiehlt auch folgende Services nicht laufen zu lassen (aus Performancegründen): DFS, Distributed Transaction Coordinator, Fax, File Replication, Indexing, ICS, Intersite Messaging, Kerberos Key Distribution, License Logging, Print Spooler, Task Scheduler, Telnet, Windows Installer.

Zusammenfassung

Main Site
1 Domain (1 Forest, 1 Tree)
Domain Controller mit Global Catalog Server
ev. DHCP Server der private IP-Nummern der Klasse B vergibt (besser statisch)
Permanente Internet Anbindung via Cablecom mit statischer IP-Nummer
ISA Server, dient als Proxy, RRAS und VPN Server für viele gleichzeitige Verbindungen

Schuleinheits-Site
Organizational Unit
Domain Controller mit Global Catalog Server
ev. DHCP Server der private IP-Nummern der Klasse B vergibt (besser statisch)
Internet Anbindung via Cablecom mit statischer IP-Nummer, Horgenberg via ISDN mit dynamischer IP-Nummer
ISA Server, dient als Proxy, RRAS und VPN Server für wenige gleichzeitige Verbindungen, Horgenberg mit demand-dialing
ev. Chained Proxy Server, falls Internet Verbindung via MainSite und Geld vorhanden

Accounts

Jede Lehrperson erhält einen eigenen Windows 2000 Account der auch einen e-mail Alias der Form

name-lehrperson@schuleinheit.schule.horgen.ch

Schüler erhalten zwecks Vereinfachung der Administration keinen eigenen Account und auch kein e-mail Postfach. Sie loggen sich ein mit dem Usernamen

klasse.name-lehrperson

Damit können Daten automatisch auf dem Server in einem Folder gespeichert werden, welche der Lehrperson zugeordnet ist. Damit hat diese die Möglichkeit die Daten zu sichten, abzuspeichern usw.

Group Policies

Es werden folgende Group Policies definiert:

1. Lehrer
2. Schüler
3. Kustoden
4. Administratoren
5. Grund-, Unter-, Mittel- und Oberstufe
6. VPN Routers
7. RAS VPN Clients

Die ersten 4 Policies dienen hauptsächlich der Konfiguration des Desktops und der Zuordnung von Permissions.
Die 5. Policy dient der Installation und zur Verfügung Stellung der stufengerechten SW.
Policies 6 und 7 dienen der Verbindung via VPN (siehe Anhang).

Die Berechtigungen für die einzelnen PCs sollen sehr restriktiv gesetzt werden, nur so kann der Wartungsaufwand niedrig gehalten werden.
Allerdings scheint es nicht zu umgehen sein, Lehrern einen gewissen Spielraum einzuräumen, indem sie z.B. individuelle Software lokal installieren können. Dies mit Einschränkungen hinsichtlich Bestandesgarantie und Support: (siehe Informatikkonzept der Primarschule Horgen, http://pit.fritz.net/schule). Für diese Installationen sollen die minimal notwendigen Rechte gewährt werden. Wie konkret beispielsweise ein Überschreiben von Dynamic Link Libraries (DLLs), die im System Ordner residieren müssen verhindert wird, ist zu überlegen.

SW Installation und Maintenance

Die MS-Tools "Windows Installer / SW Installation and Maintenance Technology" wirken auf den ersten Blick verlockend, v.a. wegen der einfachen Installation bei vorgegebenen SW-Packages und der vergebenden Installation ("Selbstheilung"). Die Erfahrung zeigt aber:

(1) zu Installation von Applikationen aufgrund von SW Packages: diese Packages sind nur so gut wie ihre Ersteller. Eine minutiöse Kontrolle einer Prototyp Installation ist unerlässlich, will man (ev. erst spätere) Auswirkungen auf andere Programme verhindern.
(2) zu Vergebende (resilient) Installationen: Bei der Wiederherstellung einer Applikation werden deren Files z.T. wieder hergestellt, auch wenn sie unterdessen schon durch neuere

Versionen ersetzt worden sind. Dies kann weder kontrolliert noch verhindert werden, da sich dieser Prozess auf dem Client PC abspielt.

(3) zu Komplette Deinstallation: Dies ist nicht von grosser Bedeutung, da Updates meist alte Versionen ersetzen, und bei kompletten Deinstallationen schlimmstenfalls ungebrauchte Registry Einträge verbleiben, die aber nicht mehr gebraucht werden und daher nichts schaden.

Angesichts dieser Erfahrungen und der beschränkten Flexibilität wird ein anderes Prozedere vorgeschlagen:

1. Installation eines Prototyps, wobei die effektive Installation auf einem Netzwerkdrive erfolgt
2. Genaue Registrierung und ev. Anpassung aller Änderungen der Registry und aller lokalen Files (z.B. Icons)
3. Logging der Installation mit Beschreibung und Versionsnummer zwecks späterer Kontrolle
4. Automatische Verteilung dieser Änderungen an die Clients via Netzwerk
5. Automatische Inventarisierung der Installation für jeden Client, damit die Geschichte jedes Clients jederzeit abgerufen werden kann.

Disk Konfiguration

Der Fixed Disk soll grundsätzlich als Basic Disk konfiguriert werden. Es sollen mind. 3 Volumes (Laufwerke mit Laufwerksbuchstaben) eingerichtet werden, mit den Namen

- System (aktive primäre Partition, Laufwerk C:)
- Benutzer Daten (extended Partition, Laufwerk D:)
- Anwendungen (extended Partition, Laufwerk E:)

Auf dem Volume "**System**" sind alle notwendigen Boot- und System-Files gespeichert, und alle lokal installierten Programme (im wesentlichen die ganze Windows SW und verschiedene Utilities im Sinne von Firmware).

User können Daten nur lokal auf dem Volume " **Benutzer Daten**“ oder auf dem **Server** ablegen. Auf dem Server wird dafür ein Shared Folder (ev. als Distributed Files System implementiert) verwendet, auf dem die Daten standardmässig direkt in einen Folder mit dem gleichen Namen wie der Username abgelegt werden. Typische Usernamen sind die Namen von Lehrpersonen, z.B. meier, oder die Usernamen welche von den Schülern benützt werden, z.B. klasse.meier. Standard-Speicherort ist dieser Folder auf dem Server und nicht der lokale Folder c:\EigeneDateien.
Der Zugriff zu allen diesen Folders ist für alle Netzwerk Benützer erlaubt, damit sie auf einfachste Weise Daten austauschen können.
In jedem dieser Folder wird zusätzlich ein Subtree namens "privat" generiert, zu dem nur die Lehrperson selbst Zugang hat.

Auf dieselbe Folderstruktur zeigt auch der **FTP-Server**. Damit kann auf dieselben Daten in der Schule via LAN und von zu Hause via Internet zugegriffen werden. Der Sicherheit des "privat" Subtrees muss im Zusammenhang mit FTP gebührend Beachtung geschenkt werden.

Alle Registryeinträge von Pfaden und Programmenu Items unter dem Startmenu werden als Kombination der Punkte 1, 3 und 6 im obigen Abschnitt *Aufruf von Programmen* in der Form

@="%LOCx%\\path\\progname"

gemacht. Um die unter *Alloziierung von Programmen* erwähnten Alloziierungsfälle 1, 2 und 3a abzudecken werden drei Environment Variable eingeführt, die an Stelle von LOCx eingesetzt werden müssen:

LOC_SERVER für Fall 1 (Programm ist immer auf einem Netzwerk-PC)
LOC_WKS für Fall 2 (Programm ist immer auf dem lokalen Volume E:), und
LOC_BOTH für Fall 3a (Programmgruppe ist entweder lokal oder auf einem Netzwerk-PC)

Es ist zu beachten, dass für die Schule Horgen der Einfachheit halber Fall 3b nicht erfüllt wird, bei dem auch einzelne Programme beliebig lokal oder auf einem Netzwerk-PC residieren können.

Beim Booten werden die Variablen LOCx initialisiert, je nachdem ein Netzanschluss besteht oder nicht:

	LOC_SERVER	LOC_WKS	LOC_BOTH
Mit Netzanschluss	Standalone DFS_Root, z.B. \\LocalDC\SrvPrograms	E:	PC spezifisch: Standalone DFS_Root (z.B. \\LocalDC\BothPrograms) oder E:
Ohne Netzanschluss	E:	E:	E:

Default für LOC_BOTH soll " Standalone DFS_Root" sein.

Es ist zu gewährleisten, dass beim Booten eines PCs ohne Netzanschluss (im Startup Script, ev. im Logon Script) die obigen Environment Variablen automatisch gemäss obiger Tabelle initialisiert werden.

Es sind also zwei DFSs Strukturen einzurichten: Die erste, "\\LocalDC\SrvPrograms", enthält alle grösseren Anwendungen. Die zweite, "\\LocalDC\BothPrograms", ist zunächst nur für zukünftige Anforderungen gedacht, und ist vorläufig leer.
Das lokale Volume E: enthält einige viel gebrauchte Utilities, und das Office-Paket. Damit ist gewährleistet, dass auch bei einem Netzunterbruch zumindest Office immer funktioniert.
Es ist zu beachten, dass die Folderstruktur auf E: genau jener der DFS Strukturen entsprechen muss. Dies gewährleistet, dass z.B. das ganze DFS "\\LocalDC\SrvPrograms" auf E: kopiert werden kann, und schon ist der PC mit allen Programmen netzunabhängig verwendbar. Natürlich können auch nur selektiv gewünschte Programme auf E: kopiert werden.

Soll ein Programm, das üblicherweise auf dem Server installiert ist, auf einem Notebook installiert werden, damit auch offline gearbeitet werden kann, so reduziert sich auf diese Weise die Installation auf eine Kopieroperation vom DFS auf das lokale Volume E:, die auch mit einem einfachen Script realisiert werden kann, so dass jede Lehrperson die "Installation" menugeführt selbst vornehmen kann.

NB: Um eine unnötige Fragmentierung des Disks zu vermeiden sollte die Grösse des Paging Files konstant gewählt werden. Richtlinie: 1.5 mal Grösse RAM.

Anhang 1: Virtual Private Network

Netzwerk Design

Die Schule Horgen schliesst 7 Primarschulhäuser und 2 Oberstufenschulhäuser ein, sowie eine Reihe von weiteren Gebäuden (z. B. Kindergärten). In 1. Priorität sollen die PS-Schulhäuser vernetzt werden und in 2. Priorität die OS-Schulhäuser. Die Anbindung der weiteren Gebäude steht zur Zeit nicht zur Diskussion, soll jedoch mit dem vorliegenden Design grundsätzlich nicht ausgeschlossen werden.

Die Vernetzung der einzelnen Schulhäuser erfolgt mit einem Virtual Private Network (VPN). Als Main Site wird (aufgrund der Anzahl Schüler und der zentralen Lage) das Schulhaus Bergli angenommen. Der Main Site ist die zentrale Verwaltungsstelle.

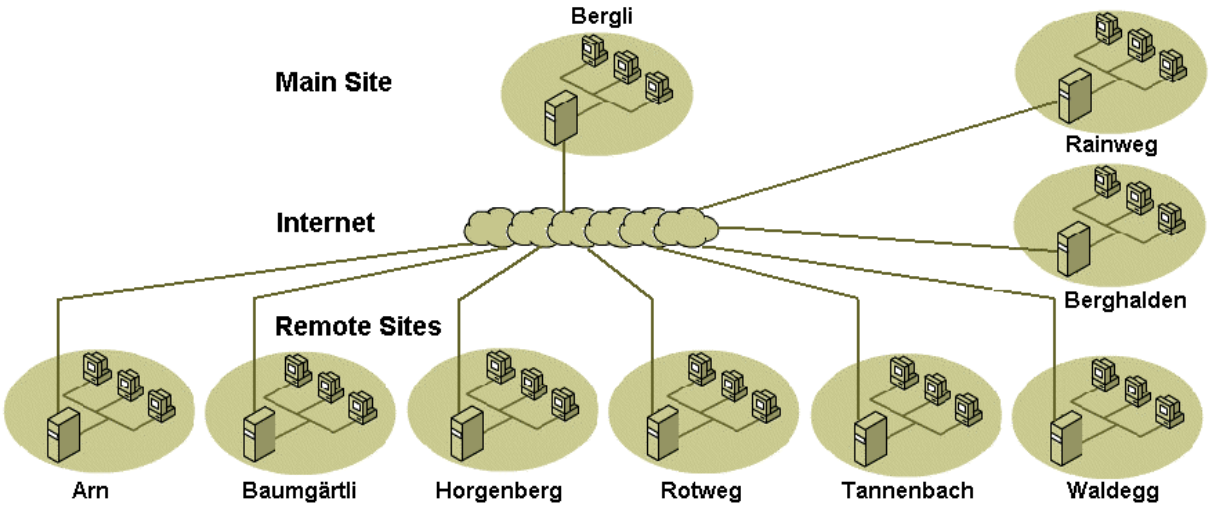

Fig. 4: Netzwerk der Schule Horgen

Wo möglich sollen die Schulhäuser via dem TV-Kabelnetz der Firma Cablecom an das Internet angeschlossen werden. Dies hat folgende Vorteile:

- Statische IP-Nummer: Um von aussen erreichbar zu sein (Wartung!) ist eine feste IP-Nummer praktisch unabdingbar.
- Dauernde Internet Verbindung, das Warten auf den Verbindungsaufbau entfällt, Resourcen sind jederzeit auch von aussen erreichbar (Wartung!).
- Grosse Verbindungsgeschwindigkeit (je nach Abonnementtyp liegt die Download Geschwindigkeit zw. 512 kbs und 2 Mbs, d.h. sie ist 8 bis 32 Mal grösser als bei (1-Kanal-) ISDN.
- Feste Kosten, die nicht wie bei ISDN von der Anschlusszeit oder wie bei xDSL vom Datenvolumen abhängen.
- Moderate Preise: Cablecom bietet für Schulen einen Rabat von 50% an, d.h. der billigste Abo-Preis beträgt Fr. 125.-/Monat.

Ohne Kabelanschluss sind zur Zeit (aber Nachbarhäuser sind angeschlossen): Schulhaus Arn und Bergli. In der Umgebung des Schulhauses Horgenberg ist kein Kabelanschluss möglich. Dies bedeutet, dass das Arn und Bergli anzuschliessen sind. Auf dem Horgenberg ist demand Dial-Up zu verwenden (ISDN schon vorhanden).

VPN Verbindung eines Remote Sites zur Main Site

Übersicht

Jede Site besteht aus einer Anzahl PCs, dem sog. remote Intranet, und einem MS-Internet Security and Acceleration (ISA) Server, welcher die Verbindung zum Internet und der Main Site (Bergli) herstellt.
Folgende Verbindungen sind möglich:

- innerhalb einer Site,
- von einer Site zu jeder anderen (via der Main Site), und
- zu einer beliebigen Internet Resource.

Nicht möglich sind direkte Verbindungen vom Internet zu einem beliebigen PC.

Intranets

Den PCs der Intranets werden private IP-Nummern zugeteilt, beispielsweise im Bereich

172.n+15.0.0 bis 172.n+15.255.255

wobei die Zahl n für jedes Schulhaus verschieden ist: n=1, 2, 3 ... 9 für das Schulhaus Bergli, Arn, Baumgärtli ... Rainweg. Die Subnet Mask ist 255.240.0.0 (240 ist binär 1111 0000) bzw. 255.255.0.0. Damit können in jedem Schulhaus 255*255 IP-Nummern benützt werden.
Die Zuteilung könnte am einfachsten via einem lokalen Dynamic Host Protocol (DHCP) Server erfolgen. Aus Sicherheits- und Kontrollgründen werden aber die IP-Nummern von Hand zugeteilt und inventarisiert, womit im Bedarfsfall rückverfolgbar ist welche Verbindung von welchem PC aus erfolgte.

Innerhalb jedes Schulhauses erfolgt ein Sub-Subnetting, indem jedem Raum die IP-Nummern

172.n+15.m.0 bis 172.n+15.m.255

zugeteilt werden, wobei m=1 ... Anzahl Räume. Die Subnet Mask ist 255.255.255.0.
Damit hat jeder Raum seinen klar zugeordneten IP-Bereich mit 255 IP-Nummern.

ISA Server

Der lokale ISA Server ist verantwortlich für die Verbindung zum Internet, insbesondere. zum Internet Service Provider (ISP), und zur Erstellung eines VPN Tunnels zur Main Site (Fig. 5).

Da der VPN Tunnel nicht direkt vom lokalen PC kommt, spricht man von einem Router-to-Router VPN. Der lokale ISA Server wird als VPN Client bezeichnet, der ISA Server auf der Main Site als VPN Server. Der Vorteil dieser symmetrischen Anordnung ist, dass VPN Verbindungen in beiden Richtungen erstellt werden können, sowie die einfache Konfiguration der PCs für alle Verbindungsarten.

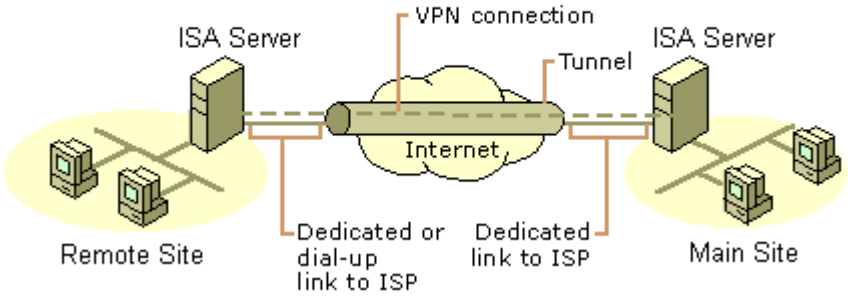

Fig. 5: Komponenten einer VPN Verbindung

Ein PC des remote Intranets kann drei mögliche Verbindungen beantragen:
1. zu einem anderen PC im selben Intranet,
2. zu einem beliebigen Server auf dem Internet,
3. zu einem PC im Intranet der Main Site der Schule Horgen.
4. zu einem PC in einem anderen Intranet der Schule Horgen.

1. Verbindung zu einem anderen PC im selben Intranet
Diese Verbindung erfolgt direkt innerhalb des Local Area Networks (LAN) des Schulhauses. Der ISA Server ist nicht involviert.

2. Verbindung zu einem beliebigen Server auf dem Internet
Es gibt zwei Möglichkeiten eine beliebige Verbindung zu einer Internet Resource herzustellen, entweder direkt, oder via eine VPN Verbindung zur Main Site.
Direkte Verbindung: Alle PCs des Intranets sind, da sie keine ISA Firewall Software installiert haben, SecureNAT Clients. Der lokale ISA Server leitet den Request eines SecureNAT Clients, d.h. eines PCs, mittels des MS-SecureNAT Protokolls transparent an den Gateway des ISP weiter. Antworten werden ebenso wieder an den PC geroutet. SecureNAT unterscheidet sich vom gewöhnlichen NAT nur durch die Möglichkeit der Anwendung von ISA-Policies auch auf SecureNAT Clients.
Verbindung via VPN: Man könnte z. B. aus Sicherheitsgründen verlangen, dass alle Internet Verbindungen über einen zentralen Proxy Server der Main Site laufen. Dies gibt zwar eine Mehrbelastung Server auf der Main Site, erleichtert aber eine zentrale Verwaltung. Die Verbindung erfolgt gleich wie im Fall 3 (siehe unten).

NB: Im Falle des Schulhauses Horgenberg ist demand Dialup via ISDN einzurichten.

3. Verbindung zu einem PC im Intranet der Main Site der Schule Horgen
Der lokale ISA Server benützt (ev. mit vorangehendem Aufbau) die VPN Verbindung zum VPN Server der Main Site.
Im Falle vom Horgenberg ist der lokale ISA Server so zu konfigurieren, dass bei einem VPN Request zuerst automatisch eine demand dialup Verbindung zum Internet bzw. ISP, erfolgt, und dann die VPN Verbindung aufgebaut wird.

Die Übertragung via VPN beruht auf einer normalen TCP Verbindung für den Tunnel und generic routing encapsulation (GRE) für die Verpackung in PPP Frames der Daten. Diese Daten können chiffriert und komprimiert werden. Die Frames werden mit privaten IP-

Adressen versehen, welche nur der ISA Server sieht und entziffert, sowie einem Header mit Public Adressen, welche das Routing über das Internet sicherstellen (Fig. 6). Die Public Adressen sind diejenigen der ISA Server (lokaler VPN Client und main VPN Server).

Die private Destination IP ist die (private) Adresse eines beliebigen PCs auf dem main Intranet (oder auf einem beliebigen anderen, nicht lokalen Intranet).

Die private Source IP braucht etwas mehr Erklärung (vgl. http://www.microsoft.com/technet/win2000/win2ksrv/reskit/intch09.asp):
Wenn ein VPN Server aufgesetzt wird, wird ein virtuelles Interface kreiert über das alle Verbindungen gehen. Eine Verbindung erfolgt also zwischen dem virtuellen Interface des VPN Clients und dem virtuellen Interface des VPN Servers. Die Zuordnung von IP Nummern zu diesen virtuellen Interfaces erfolgt durch den VPN Server. Er holt sie entweder dynamisch von einem DHCP Server oder aus einem statischen Pool von Adressen, die bei seiner Konfiguration definiert wurden. Sie können public oder privat sein.
Daten werden demzufolge von der virtuellen Client Adresse zur (privaten) Adresse im main Intranet geschickt. Der VPN Client ornet die virtuelle Client Adresse der IP Adresse des anfragenden PCs. Der VPN Server findet den PC im main Intranet aufgrund seiner Local Address Tabel (LAT). Ebenso findet müssen in dieser LAT auch alle Adressen des Remote Intranets definiert sein, damit Anfragen von PCs im main Intranet weitergeleitet werden können.

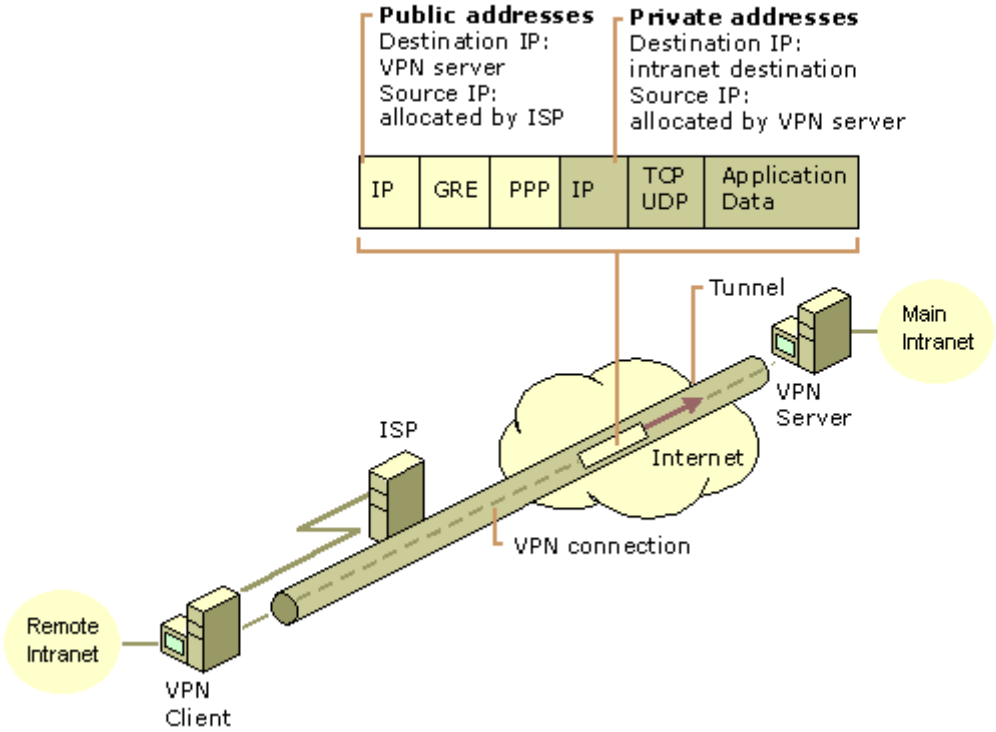

Fig. 6: Komponenten einer VPN Verbindung

4. Verbindung zu einem PC in einem anderen Intranet der Schule Horgen
Dieser Verkehr wird minimal sein. Darum und aus Sicherheitsüberlegungen werden solche Verbindungen zuerst via VPN an die Main Site gemacht, von wo sie mit einer anderen VPN Verbindung automatisch? zum anderen Intranet weitergeleitet werden (Fig. 7).

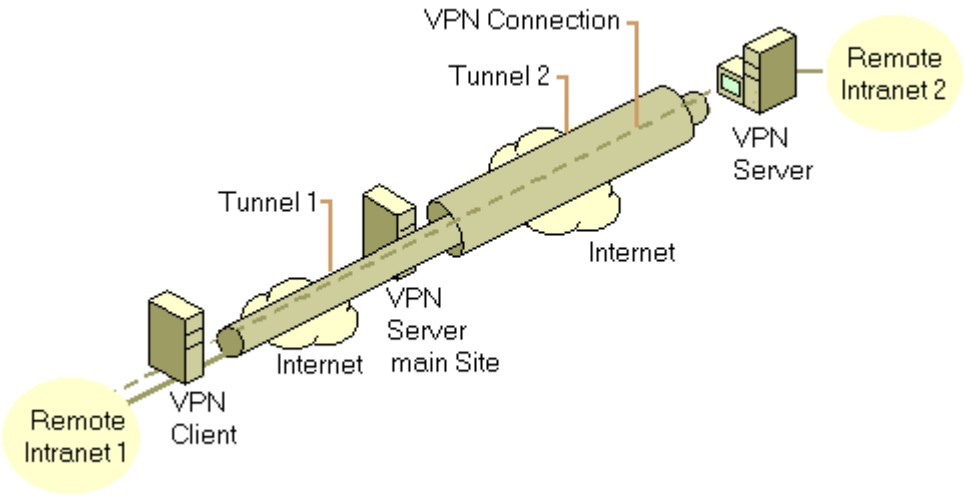

Fig. 7: VPN Verbindung von einem Intranet zu einem andern

Konfiguration der ISA Server

Einleitung

Beispielhaft soll hier die Konfiguration der ISA Server auf dem main Site und einem remote Site erklärt werden (vgl. auch http://www.microsoft.com/WINDOWS2000/library/howitworks/communications/remoteaccess/w2kvpnscenario.asp und http://mspress.microsoft.com/it/feature/020101.htm).
Der main Site benütze für sein Intranet das private Netzwerk 172.18.0.0 mit der Subnet Mask 255.240.0.0. Von ISP erhalten: IP Nummer 62.2.116.3. Aufrufbar auch via Domain Name schule.horgen.ch.

Die remote Sites benützen für ihr Intranet das private Netzwerk 172.n+15.0.0 mit der Subnet Mask 255.240.0.0, wobei n aus untenstehender Tabelle hervorgeht. Der Gateway für die PCs der remote Sites ist jeweils der interne LAN Adapter des lokalen ISA Servers, d.h. 172.n+15.0.1

Site Nummer n	Schuleinheit	Subnet	Gatway
1	Arn	172.16.0.0	172.16.0.1
2	Baumgaertli	172.17.0.0	172.17.0.1
3	Main Site Bergli	172.18.0.0	172.18.0.1
4	Horgenberg	172.19.0.0	172.19.0.1
5	Rotweg	172.20.0.0	172.20.0.1
6	Tannenbach	172.21.0.0	172.21.0.1
7	Waldegg	172.22.0.0	172.22.0.1

Konfiguration des ISA Servers der main Site

Konfiguration des LAN und WAN Adapters

Der LAN Adapter erhält die Adresse 172.18.0.1 mit der Subnet Maske 255.255.0.0.
Der WAN Adapter 62.2.116.3 mit der Subnet Mask 255.255.255.255.

Accounts

Groups: Create
- VPN_Users: used for RAS connections
- VPN_Routers: used for router-to-router VPN connections

Accounts: Create
- VPN_MainSite, and add it to group VPN_Routers.
- VPN_xyz, where xyz=Arn, Baumgärtli ... Rainweg,
  set dial in properties to Control Access through Remote Access Policy,

Add above accounts to group VPN_Routers.
Add all other accounts to group VPN_ Users.

Policy

Die default policy wird ersetzt durch eine Policy namens "VPN Routers":

Conditions: Port Type VPN
- Windows Group is VPN_Routers
- Called Station is 62.2.116.3 (damit werden nur Tunnels vom Internet erlaubt, aber nicht vom Main Site Intranet).

Permissions: Grant Remote Access.
Profile Settings: Extensible Authentication und MS Encrypted Authentication v.2 and original. Nur strong oder strongest Encryption sind zulässig.

Füge eine Policy hinzu namens "RAS VPN Clients":

Conditions: Port Type VPN
- Windows Group is VPN_ Users
- Called Station is 62.2.116.3 (damit werden nur Tunnels vom Internet erlaubt, aber nicht vom Main Site Intranet).

Permissions: Grant Remote Access.
Profile Settings: Extensible Authentication und MS Encrypted Authentication v.2 and original. Nur strong oder strongest Encryption sind zulässig.

IP Address Pool

Es werden 253 statische Adressen für maximal 253 Verbindungen von VPN Clients definiert:
172.18.255.1 bis 254

Demand Dial Interface to Baumgaertli Site

Interface Name: VPN_**Baumgaertli**
Destination Address: 62.2.116.**2**
Connect using VPN, VPN Type is PPTP, route IP packets
Dial out credentials: Username: VPN_MainSite
Properties: Persistent connection.
Static route to Intranet at Baumgaertli
Interface: VPN_ **Baumgaertli**
Destination Address: 172.**17**.0.0
Network Mask: 255.240.0.0
Metric: 1

Demand Dial Interface zu den anderen Sites

Die fetten Zeichen im oberen Abschnitt werden durch die entsprechenden ersetzt für Arn, Baumgärtli ... Rainweg. Horgenberg braucht nur Static Routes, aber kein Dial Interface.

Konfiguration des ISA Servers der remote Sites (ausser Horgenberg)

Die remote Sites benützen für ihr Intranet das private Netzwerk 172.n+15.0.0 mit der Subnet Mask 255.240.0.0.
Im folgenden wird die Konfiguration für die Schuleinheit Baumgärtli (n=2) erläutert, d.h. das Netzwerk 172.17.0.0.
Von ISP erhielt das Baumgärtli die IP Nummer 62.2.116.2.

Konfiguration des LAN und WAN Adapters

Der LAN Adapter erhält die Adresse 172.17.0.1 mit der Subnet Maske 255.255.0.0.
Der WAN Adapter 62.2.116.2 mit der Subnet Mask 255.255.255.255.

Policy

Die default policy wird ersetzt durch eine Policy namens "VPN Routers":

Conditions: Port Type VPN
Windows Group is VPN_Routers
Called Station is 62.2.116.2 (damit werden nur Tunnels vom Internet erlaubt, aber nicht vom Baumgärtli Intranet).
Permissions: Grant Remote Access.
Profile Settings: Extensible Authentication und MS Encrypted Authentication v.2 and original. Nur strong oder strongest Encryption sind zulässig.

IP Address Pool

Es werden 5 statische Adressen für maximal 5 Verbindungen von VPN Clients definiert:
172.17.255.1 bis 5

Demand Dial Interface to VPN Server at main Site

Interface Name: VPN_MainSite
Destination Address: 62.2.116.3 (schule.horgen.ch)
Connect using VPN, VPN Type is PPTP, route IP packets
Dial out credentials: Username: VPN_Baumgaertli, Domain: schule.horgen.ch
Properties: Persistent connection.
Static route to VPN Server at main Site
Interface: WAN Adapter to ISP
Destination Address: 62.2.116.3 (schule.horgen.ch)
Network Mask: 255.255.255.255
Gateway: 0.0.0.0 (due to PP-connection to ISP, any address is valid)
Metric: 1
Static route to Intranet at main Site (nur notwendig, falls Intranet der main Site andere Adressen hat als andere Intranets).
Interface: VPN_MainSite
Destination Address: 172.18.0.0
Network Mask: 255.240.0.0
Metric: 1

Static route to all other Intranets
Interface: VPN_MainSite
Destination Address: 172.18.0.0
Network Mask: 255.240.0.0
Metric: 1

Konfiguration des ISA Servers der remote Site Horgenberg

Der Unterschied vom Horgenberg zu den anderen Sites besteht darin, dass der Horgenberg via ISDN mit dem Internet verbunden ist. Dies bedeutet, dass er bei jedem Verbindunhsaufbau eine andere IP Nummer erhält. Deshalb wird der Horgenberg so konfiguriert, dass nur ein Verbindungsaufbau vom Horgenberg zur Main Site möglich ist, aber nicht umgekehrt.

Das Netzwerk Horgenberg hat die Nummer 172.19.0.0 mit der Subnet Mask 255.240.0.0.

Konfiguration des LAN und WAN Adapters

Der LAN Adapter erhält die Adresse 172.19.0.1 mit der Subnet Maske 255.255.0.0.
Der WAN Adapter erhält seine Nummern automatisch vom ISP.

Policy

Die default policy wird ersetzt durch eine Policy namens "VPN Routers":

Conditions: Port Type VPN
Windows Group is VPN_Routers
Called Station is 62.2.116.3 (schule.horgen.ch) (damit werden nur Tunnels vom Internet erlaubt, aber nicht vom Baumgärtli Intranet).
Permissions: Grant Remote Access.
Profile Settings: Extensible Authentication und MS Encrypted Authentication v.2 and original. Nur strong oder strongest Encryption sind zulässig.

IP Address Pool

n.a.

Demand Dial Interface to VPN Server at main Site

Interface Name: ISP
Destination Address: Phone No. of ISP
Connect using ISDN, route IP packets
Dial out credentials: Username: ISP Account
Static route to VPN Server at main Site
Interface: WAN Adapter to ISP
Destination Address: 62.2.116.3 (schule.horgen.ch)
Network Mask: 255.255.255.255
Gateway: 0.0.0.0 (due to PP-connection to ISP, any address is valid)
Metric: 1
Interface Name: VPN_MainSite
Destination Address: 62.2.116.3 (schule.horgen.ch)
Connect using VPN, VPN Type is PPTP, route IP packets
Dial out credentials: Username: VPN_Baumgaertli, Domain: schule.horgen.ch
Properties: Persistent connection.

Static route to VPN Server at main Site
Interface: WAN Adapter to ISP
Destination Address: 62.2.116.3 (schule.horgen.ch)
Network Mask: 255.255.255.255
Gateway: 0.0.0.0 (due to PP-connection to ISP, any address is valid)
Metric: 1
Static route to Intranet at main Site (nur notwendig, falls Intranet der main Site andere Adressen hat als andere Intranets).
Interface: VPN_MainSite
Destination Address: 172.18.0.0
Network Mask: 255.240.0.0
Metric: 1
Static route to all other Intranets
Interface: VPN_MainSite
Destination Address: 172.18.0.0
Network Mask: 255.240.0.0
Metric: 1

Konfiguration eines PCs eines Remote Access Users

Use „Make New Connection“ wizard:
Hostname: 62.2.116.3 (schule.horgen.ch)
VPN Connection settings:
Type of called dialup server: PPTP, route IP packets
Dial out credentials: Username: xyz, Domain: schule.horgen.ch

Anhang 2: Offerte Kabelanschluss

Cablecom Media AG
Carrier Solutions
Zollstrasse 42
CH-8021 Zürich
Telefon : 0800 888 300
Telefax : 0800 888 301
E-Mail : business@cablecom.ch
URL : www.cablecom.net

Webcom Schulpreisliste

	WEBCOM LIGHT	WEBCOM BASIC	WEBCOM STANDARD	WEBCOM PRO
Bandbreite (Down-/Upstream)	512/128 Kb/s	512/256 Kb/s	1024/256 Kb/s	2048/512 Kb/s
Accesstechnologie	Cablemodem	Cablemodem	Cablemodem	Cablemodem
Hosting	www.IhrName.ch	www.IhrName.ch	www.IhrName.ch	www.IhrName.ch
DNS Einträge	Inbegriffen	Inbegriffen	Inbegriffen	Inbegriffen
Statische IP	1x Inbegriffen	5 x Inbegriffen	5 x Inbegriffen	13 x Inbegriffen
Diskspace	5 MB	20 MB	50 MB	100 MB
E-Mail Accounts	1	10	25	50
Anzahl Rechner	keine Limite	keine Limite	keine Limite	keine Limite
First Level Support	8.00 - 20.00	8.00 - 20.00	8.00 - 20.00	8.00 - 20.00
Normalpreis/Monat	**sFr. 250.00**	**sFr. 450.00**	**sFr. 650.00**	**sFr. 950.00**
Abzüglich 50% Rabatt	- sFr. 125	- sFr. 225.-	- sFr. 325.-	- sFr. 475.-
Schulpreis/Monat	**sFr. 125.00**	**sFr. 225.00**	**sFr. 325.00**	**sFr. 475.00**

Innerhalb der einzelnen Webcom Abos ist ein Upgrade der E-Mail Alressen sowie des Diskspace jederzeit möglich.
Bitte verlangen Sie die Preisliste für die Webcom Upgrades.