Dr. Suppan International Institute

Der Netzwerk Insider

Juni 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

VPN mit Windows 2000

von Alexander Zarenko

Das Thema Virtual Private Networking (VPN) ist in aller Munde, in immer mehr Unternehmen wird derzeit über den Einsatz von VPN-Technologien nachgedacht oder es sind bereits Lösungen implementiert.

Hauptsächlich entstehen solche Lösungen aufgrund von Anforderungen, verschiedene Standorte kostengünstig miteinander zu verbinden oder Mitarbeitern den Zugriff auf Ressourcen des Unternehmens zu gewähren – möglichst von überall in der Welt. Bisher wurden für Standortverbindungen meist Standleitungen gemietet und Direkteinwahl per RAS mit Modems oder ISDN-Adaptern betrieben, um den gewünschten Remote-Zugriff zu ermöglichen. Mit dem Siegeszug des Internets wurde dieses Medium jedoch auch für derartige Anforderungen interessant. Dies hat u.a. folgende Gründe:

- Nahezu weltweite Verfügbarkeit des Internet
- Unabhängigkeit von der Einwahltechnik (z.B. ISDN nicht flächendeckend verfügbar)
- Keine Einwahl-Hardware im Unternehmen erforderlich (Modem-Pools o.ä.)
- Geringe Verbindungskosten – es ist nur der Weg zum nächstgelegenen Internet Service Provider (ISP) zu bezahlen, keine teuren Standleitungen zwischen den Standorten nötig, keine Ferngesprächsgebühren für Remote-Access-Clients.

Licht und Schatten
für Virtual Private Networking
mit Windows 2000

Es gibt jedoch auch Schattenseiten:

- Das Internet ist ein öffentliches Medium – Vertraulichkeit und Integrität der übermittelten Daten sind nicht gewährleistet.
- Die Verfügbarkeit kann sehr stark schwanken, Engpässe sind teilweise an der Tagesordnung.

Zum Schutz von Vertraulichkeit und Integrität der Daten sind im Laufe der Zeit verschiedene Verfahren entwickelt worden, die von aktuellen VPN-Lösungen genutzt werden.

Vor Verfügbarkeitsschwankungen bzw. Engpässen bezüglich der zur Verfügung stehenden Bandbreite kann man sich jedoch nur sehr eingeschränkt schützen. Beispielsweise bietet sich hier an, einen einheitlichen Provider für alle Zugänge zu nutzen, wobei selbst dieser Ansatz in der Regel keine Garantien seitens des Providers mit sich bringt. Eine beliebte Lösung zur Bildung eines VPN über das Internet stellt der Einsatz von Firewalls dar, die über eine VPN-Komponente verfügen. Zur Netzkopplung werden hierbei ein oder mehrere Tunnel zwischen verschiedenen Firewalls etabliert, für den Remotezugriff üblicherweise Tunnel zwischen den Remote-Clients und der Firewall, die von den Clients initiiert werden. Als Tunnelprotokoll wird in beiden Fällen meist IPSec im ESP-Tunnelmodus eingesetzt.

Der Einsatz von Firewalls oder auch Routern als VPN-Gateway ist jedoch nicht die einzige Möglichkeit.

Dieser Artikel betrachtet die Möglichkeiten unter Windows 2000 für ein Design und den Aufbau eines VPN-Verbundes. Dabei werden sowohl die Möglichkeiten als auch die Grenzen aufgezeigt.

weiter Seite 8

Zum Geleit

Cat 5-Qualität ist unzureichend !

Lokale Netzwerke werden in den nächsten 3 - 5 Jahren noch einmal einen erheblichen Leistungssprung machen.

Wesentliche Träger dieser Entwicklung sind einerseits die massiven Zentralisierungs-Tendenzen, die von den neuen Speicher- und Server-Technologien ausgehen, und andererseits die erhöhten Verfügbarkeits-Anforderungen, die aus den Bereichen Server-Technologien und Voice-over-IP stammen. Speziell die Zentralisierung, die mit zentralem Speicher und Leistungs-Clustern einher geht, wird zu einem Sprung in den Kapazitäten Lokaler Netze von mindestens Faktor 10 führen.

Naturgemäß führt diese Entwicklung zu der Frage, ob unsere Infrastrukturen darauf vorbereitet sind. Mindestens im Kabelbereich muss dies bezweifelt werden. Immer noch wird zum Beispiel im Tertiärbereich von vielen Gesprächspartnern eine vorhandene Cat-5-Verkabelung als Qualitäts-Maßstab angesehen. Dabei ist festzustellen:

- Die Kategorie-5-Leistungsmerkmale reduzieren sich auf eine 4-adrige Übertragung.
- Innerhalb dieser werden lediglich Dämpfung und Nebensprechen als Maßstab definiert.

Gigabit-Ethernet wird zweifelsfrei innerhalb der nächsten drei Jahre auch verstärkt im Endgerätebereich eingesetzt werden. – Man beachte alleine die Preisentwicklung der Gigabit-Technologie, Gigabit-NICs für Twisted Pair werden in 3 Jahren maximal noch 100 DM kosten und damit völlig unabhängig von der Bedarfsfrage diese Technologie durchsetzen. Hinzu kommt, dass mit zunehmender Zentralisierung von Servern und Speichern die sogenannte Lokalität im Sinne der messtechnischen Performance der entsprechenden Verbindungen zwischen Endgeräten und Zentralsystemen nur erhalten werden kann, wenn der Umstieg auf Gigabit erfolgt. – Gigabit-Ethernet basiert auf einer 8-adrigen, bidirektionalen Übertragung, deren qualitative Umsetzung völlig neue Leistungsmerkmale von Kabeln erfordert.

weiter Seite 2

Cat 5-Qualität ist unzureichend!

Fortsetzung von Seite 1

Dementsprechend wurden der EIA/TIA 568- und der EN50173-Standard im letzten Jahr an diese neue Situation angepasst. EIA/TIA definiert den Cat 5e-Standard, die EN50173 eine überarbeitete Class D.

Speziell hier liegt das Problem. Die meisten Anwender haben nicht bemerkt, dass sich der deutsche Verkabelungs-Standard verändert hat, da er scheinbar genau so heißt wie zuvor.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Dementsprechend ist der Sprengstoff, der in diesem aktuellen und für Deutschland verbindlichem Standard enthalten ist, offensichtlich nur wenigen Betroffenen aufgefallen.

Ein typisches Problem liegt dabei in der Einführung der Messung der Übertragungsstrecke, bestehend aus Endgeräte-Anschlusskabel, Dose im Kabelkanal, fest verlegten Kabel, Rangierfeld, Rangierkabel. Eine Messung dieser Strecke wird durch die aktuelle EN 50173 vorgeschrieben. Was bedeutet dies in der Praxis ?

- Zuerst einmal kann davon ausgegangen werden, dass die meisten Anwender alle vorhandenen Rangier- und Anschlusskabel wegwerfen und durch neue ersetzen müssen.

- Dann wird durch die Messung ein ganz bestimmtes Rangier- und Anschlusskabel an ein festes installiertes Kabel gebunden. Dies würde bedeuten: Nummerierung aller derartiger Kabel, Aufbau einer Bestands- und Messdatenbank etc., keine Verwechslung zwischen Kabeln, keine Rückwärtskompatibilität.

Damit nicht genug. Weder die aktuelle Cat 5e noch die aktuelle EN50173 sind ein Garant für Gigabit-Fähigkeit. Beide lassen auf längeren Installationswegen Bitfehler erwarten, die für Voice-over-IP oder zum Beispiel Multicast-Anwendungen tödlich sein könnten. Dementsprechend sind die noch nicht verabschiedeten Cat 6 und Class E-Standards eigentlich das Maß der Dinge. Deren Leistungswerte sind auch relativ stabil, so dass man sich an diesen orientieren kann.

Aber: eine ganze Reihe bestehender Produkte erfüllt diese Leistungswerte zur Zeit nicht.

Um diese Situation nicht noch weiter zu verschlimmern, werden Diskussionen darüber geführt, ob nicht alle Stecksysteme einer Verbindung inkl. Rangier- und Anschlusskabel von einem Hersteller sein müssen. Eine Forderung, die in der Praxis absolut undurchsetzbar ist.

Spannend wird die Sache nun dadurch, dass die notwendige Messtechnik zur Prüfung einer bestehenden Verkabelung offensichtlich bis Anfang des Jahres mehr eine Schätztechnik war. Immerhin streuten die Werte einer 30-mal durchgeführten Messung ohne Veränderung des Messaufbaus um über 25%. Sprich: der Installateur muss nur solange messen bis ein "Passed" erscheint.

Um die ganze Angelegenheit abzurunden, verschärft sich der Streit um das Thema UTP kontra S-UTP/S-STP. Seit neuestem werden in der ISO-Normung Messverfahren zur Prüfung der Schirmungsqualität diskutiert. Dem steht die Potential-Problematik einer Schirmung gegenüber.

Diesen ganzen Problemkreis haben wir für Sie aufgearbeitet:

- Wir haben Produkte verschiedener Hersteller installiert und auf Class-E vermessen.

- Wir haben Produkte gemischt.

- Wir haben die neueste Messtechnik eingesetzt und auf Nutzbarkeit geprüft.

- Wir haben den aktuellen Stand der Normung zusammen mit dem deutschen Vertreter bei der ISO aufgearbeitet.

- Wir haben klare Empfehlungen zur Realisierung einer neuen Verkabelung erarbeitet.

- Wir haben klare Empfehlungen zur Prüfung und Überarbeitung bestehender Verkabelung erarbeitet.

- Wir haben den Problembereich Potential aufgearbeitet.

Das Ergebnis präsentieren wir Ihnen in Form des Verkabelungs-Forums 2001, vom 24. bis 26. September in Königswinter. Natürlich sind auch die bestehenden Kontrahenten des Marktes eingeladen. So erwarten wir mit Spannung eine kontroverse, aber informative Veranstaltung.

Ihr
Dr. Jürgen Suppan

Neues Seminar

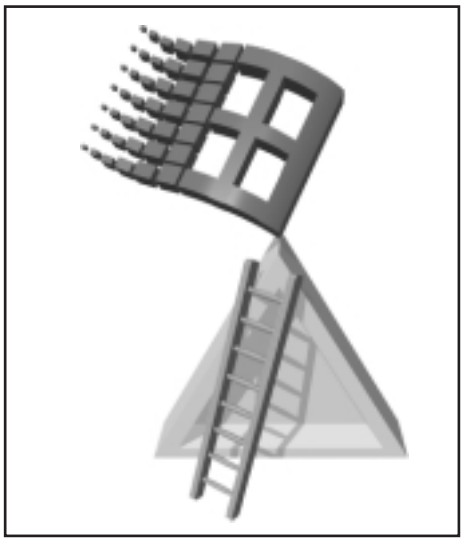
Migration zu Windows 2000 Active Directory

Vom 27. bis 28. September 2001 veranstaltet die ComConsult Akademie im Holiday Inn in Bonn zum ersten Mal ihr neues Seminar "Migration zu Windows 2000 Active Directory" für Planer, Betreiber und Anwender von Unternehmensnetzen.

In diesem Seminar lernen die Teilnehmer verschiedene Migrationsansätze zu klassifizieren, welchen Migrationsansatz Sie verwenden sollten, welche Tools äußerst hilfreich bei der Migration sind und wie und in welcher Form Sie diese Tools einsetzen können.

Am ersten Tag vermittelt das Seminar die grundsätzlich möglichen Ansätze und gibt klare Empfehlungen für die verschiedenen Konstellationen. Diese Ansätze sind nicht nur für die Migration von Windows NT 4.0 auf Windows 2000 geeignet, aber auf dieses Migrationsbeispiels baut das Seminar auf. Da in der Praxis ein gemeinsamer Einsatz von Windows NT 4.0 und Exchange sehr häufig ist, wird das Thema Exchange ebenfalls berücksichtigt.

Am zweiten Tag des Seminars werden insbesondere zwei entscheidende Migrationskomponenten detailliert erläutert und demonstriert: das Active Directory Migration Tool (ADMT) und der Active Directory Connector (ADC). Dieser Teil ist extrem praxisbezogen, da die Referenten diese Tools bei Migrationen einsetzen bzw. eingesetzt haben. Für diejenigen, die eine Migration von NT 4.0 auf Windows 2000 oder von NT 4.0 mit Exchange auf Windows 2000 anstreben, ist dieses Seminar die ideale Basis.



Die Referenten sind Spezialisten aus dem Kompetenz Center Backoffice der ComConsult Beratung und Planung GmbH.

Markus Holländer, MCSD, besitzt langjährige Projekterfahrung im Design und im Betrieb von Windows NT und Windows 2000, sowie weiterer Backoffice Produkte. In den letzten Jahren hat er zahlreiche Projekte privater und öffentlicher Auftraggeber in diesem Umfeld erfolgreich geleitet.

Dipl.-Inform. Michael van Laaks Schwerpunkte in der Konzipierung und Umsetzung von Migrationsprojekten auf Windows NT 4 und Windows 2000 sind Domänen-, IP-Management- und (Fern-) Administrationskonzepte.

Markus Holländer

Michael van Laak

"plan – build – run" Windows 2000 Active Directory Seminarreihe

Der Windows 2000 Server beinhaltet eine Reihe von sehr leistungsstarken Möglichkeiten, den Betrieb von Servern und TCP/IP-Netzen zu vereinfachen und zu signifikanten Kosteneinsparungen zu kommen. Eine Reihe von sehr erfolgreichen Projekten hat bestätigt, dass hier ein erhebliches Potenzial gegenüber den bisherigen Lösungen besteht.

Das eigentlich neue und somit auch der Grund für die vielen Vorteile, die Windows 2000 betriebstechnisch bietet, ist die Kombination einer Reihe von Verwaltungsdiensten mit einem zentralen Directory Service mit einer gleichzeitigen Integration in eine TCP/IP-Kommunikationswelt. Um die gegebenen Vorteile nutzen zu können, sind detallierte Kenntnisse einerseits der Technik des Windows 2000 Directory Services und andererseits seiner methodischen Nutzung erforderlich. Zur Vermittlung dieser Kenntnisse haben wir eine komplette Seminarreihe konzipiert, die mit aufeinander aufbauenden Seminaren aus der Planung und Konzeptionierung bis zum Betrieb von Windows 2000 Active Directory führen.

Im einzelnen besteht die Windows 2000 Active Directory Seminarreihe aus den Seminaren:

1. DNS-/IP-Design für Windows 2000 Active Directory
2. Design Windows 2000 Active Directory
3. Migration zu Windows 2000 Active Directory
4. Betrieb von Windows 2000 Active Directory

Die Seminare sind grundsätzlich unabhängig voneinander, jedoch ist es von Vorteil, wenn bei der Teilnahme an mehreren Seminaren die Reihenfolge eingehalten wird.

Windows 2000 Active Directory

Migration zu Windows 2000 Active Directory
Inhaltlicher Aufbau

Grundsätzliche Ansätze

Update der bestehenden Welt
• Wie wird das Update durchgeführt, welche Kriterien sind zu beachten hinsichtlich:
– Benutzern – Gruppen – Rechten – Profile – Richtlinien – Dienstkonten – Vertrauensstellungen
• Vor- und Nachteile dieses Ansatzes • Konstellationen bei denen ein Update empfohlen wird

Gleichzeitiger Aufbau der neuen Welt in der bestehenden Umgebung
• Wie erfolgt der parallele Aufbau, welche Kriterien sindzu beachten hinsichtlich:
– Benutzern – Gruppen – Rechten – Profilen – Richtlinien – Dienstkonten – Vertrauensstellungen – Postfächern
• Vor- und Nachteile dieses Ansatzes • Konstellationen bei denen ein Update empfohlen wird

Unabhängiger Aufbau der neuen Welt parallel zur bestehenden Umgebung
• Was ist grundsätzlich zu beachten?
• Wie stelle ich den parallelen Betrieb sicher?
• Welche Kriterien sind hinsichtlich folgender Punkte zu beachten:
– Benutzern – Gruppen – Rechten – Profilen – Richtlinien – Dienstkonten – Vertrauensstellungen – Postfächern
• Vor- und Nachteile dieses Ansatzes • Konstellationen bei denen ein Update empfohlen wird

Besonders empfehlenswerte Tools für die Migration
• ADMT - Active Directory Migration Tool: Detaillierte Vorstellung des Tools, Demonstration an einer Vielzahl von Beispielen
• ADC - Active Directory Connector:Detailierte Vorstellung des Connectors, Demonstration an einer Vielzahl von Beispielen
• Welche Tools sind ggf. noch zu empfehlen.

ComConsult Akademie – Telefax: 02408/955-399

Fax-Antwort
Windows 2000 Active Directory

☐ Ich melde mich an zum Seminar
Migration zu
Windows 2000 Active Directory
☐ 27. - 28.09.01 ☐ 26. - 27.11.01
zum Preis von EUR 1.290,-- zzgl. MwSt.

☐ Ich buche die Seminarreihe
plan - build - run
Windows 2000 Active Directory
zum Paket-Preis von EUR 4.990,--
zzgl. MwSt. (statt regulär EUR 5.760,--)
1. ☐ 04. - 06.09.01 ☐ 24. - 26.09.01
2. ☐ 18. - 20.06.01 ☐ 05. - 07.11.01
3. ☐ 27. - 28.09.01 ☐ 26. - 27.11.01
4. ☐ 01. - 02.10.01 ☐ 06. - 07.12.01

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Bonn (Übern./Frühst. DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

☐ Senden Sie mir bitte unverbindlich detailliertes Informationsmaterial über die vier Seminare der **plan - build - run Windows 2000 Active Directory** -Seminarreihe:
1. DNS-/IP-Design für Windows 2000 Active Directory
2. Design Windows 2000 Active Directory
3. Migration zu Windows 2000 Active Directory
4. Betrieb von Windows 2000 Active Directory zu

Name _____ Vorname _____

Firma, Abteilung _____ Position, Funktion _____

Abteilung _____ Funktion _____

Straße _____ PLZ, Ort _____

Telefon _____ Fax _____

eMail _____ Unterschrift _____

xDSL: Technik und Nutzen des neuen Weitverkehrs-Standards

Turboauffahrt für die Datenautobahn! – eine Goldmine für Kupfer!

Ein Erlebnisbericht von xDSL-Seminar-Teilnehmer Walter Tietz

Slogans wie in der Überschrift fand man in der Vergangenheit häufig zu dem genannten Thema. Sie waren in Richtung zum Endanwender oder in Richtung zu Herstellerfirmen formuliert.

Dem Endanwender eröffnet doch die erfolgreiche Anwendung der genannten Technik endlich ein schnelles Surfen im Internet. Da fängt es an Spaß zu machen! Und Netzanbieter wittern neue Umsatzfelder. Wer vielleicht selbst als Anbieter von unterstützenden Programmen oder Geräten auftreten will, sollte sich wohl auch besser mit den Zusammenhängen vertraut machen. Noch vor etwa einem Jahr gab es Meldungen, dass bei den etablierten Carriern wenig Interesse an ADSL bestände und der europäische Markt nur sehr langsam wachsen werde. Der Trend scheint sich umgekehrt zu haben. Auch aus Ländern jenseits von Europa (wie z.B. USA und Japan) hört man von zunehmender Verbreitung.

Telekom nennt für ihr Angebot T-DSL schon eine große Flächenabdeckung (etwa 80 %) und rasch wachsende Teilnehmerzahlen. Die Wettbewerber von Telekom schlafen auch nicht und haben in Ihre Angebote entsprechende "Bonbons" aufgenommen. Den Ort für ein Seminar mit einem solchen Thema zu finden, erfordert schon etwas Geschick. Darmstadt schien wohl dem Veranstalter ein geeigneter Ort zu sein. (Ein Vorläufer vor geraumer Zeit in Bonn war sehr gut besucht). Der Veranstalter ist ja ein sehr erfahrener Anbieter von Seminaren der verschiedensten Art.

Darmstadt als "Wissenschaftstadt" und Heimat etlicher Firmen und Organisationen rund um IT und Kommunikation hat wohl auch ein entsprechendes Potential an Interessenten zu bieten, ohne dass die eine oder andere Veranstaltung mit dem Thema xDSL darunter leidet. So finden eigentlich häufig interessante Veranstaltungen das Interesse von Firmen und Organisationen, Anwendern oder Studenten, trotz paralleler Termine (die sich ja nie ganz ausschließen lassen). Ob man denn dabei auch daran gedacht hat, dass gerade an denselben Tagen in Darmstadt die Hochschul- und Informationstage (hobit) stattfanden? Aber offenbar hat dies dem Interesse nicht geschadet, denn 23 Teilnehmer fanden sich ein, um sich "schlau" machen zu lassen. Und sie waren

"konnte die Zuschauer über die vielen Stunden fesseln": Referent Ralf Boden

beileibe nicht nur aus Darmstadt, sondern reisten von weit her an. Das Spektrum des Seminars war wohl absichtlich breit angelegt. Die Zusammensetzung der Zuhörer kamen daher auch aus den unterschiedlichsten Bereichen. Der Referent fand den richtigen Ton und konnte die Zuhörer über die vielen Stunden fesseln.

Die kompetenten Ausführungen wurden der Ankündigung gerecht. Die Seminarunterlagen waren gut aufbereitet. Es gab sogar eine CD mit PDF-Dateien der Folien!

Jeder dürfte sich das Quentchen an Information aus dem großen Angebot haben heraussuchen können, das für ihn von Bedeutung ist. Es ist ja ein alter Hut: Je besser Hersteller, Anbieter und Anwender informiert sind, desto wirkungsvoller wird sich auch eine solche neue Technik durchsetzen. Und, an der Durchsetzung dürfte es nach den letzen Stand der Meldungen über die Verbreitung keinen Zweifel mehr geben.

Der große Packen Information war gut angerichtet, wie das ausgezeichnete Buffet beim Mittagessen, das auch zur guten Stimmung beigetragen hat. Eine "Happy Hour" am ersten Abend trug sicherlich ebenfalls zum Gelingen der Veranstaltung bei.

Eine Schlagzeile dieser Tage "Kein Strom in Kalifornien" trat für die Teilnehmer wahrscheinlich etwas in den Hintergrund. Obwohl - Ohne Strom liefe auch bei uns nichts mehr, auch nicht xDSL.

xDSL: Technik und Nutzen des neuen Weitverkehrs-Standards

xDSL:Technik und Nutzen des neuen Weitverkehrs-Standards
Inhaltlicher Aufbau

Neue Marktchancen durch xDSL
- die wichtigsten Markttrends im TK- und IT-Sektor
- die heutige Technik und ihre Probleme
- Breitbandanwendungen und ihre Anforderungen
- Beispiele: Fast Internet Access, LAN-Kopplung, VoIP
- Was bietet xDSL?
- Wer sind die potentiellen Anwender?
- Business-Analyse für verschiedene Marktsegmente

Vorstellung und Bewertung alternativer Ansätze
- Stärken und Schwächen der xDSL-Technik
- Fiber to the Home (FTTH), Kabelfernsehnetze, Powerline, Wireless Local Loop (WLL) und Satellitenübertragung als mögliche Alternativen
- Welche Technologie wird in der Zukunft dominieren?

Einführung in die xDSL-Technik
- Systemkonfigurationen von ADSL, SDSL und VDSL
- Vorstellung der Hauptfunktionsblöcke
- Kanalcodierungstechniken (CRC, FEC, Interleaving)
- die häufigsten Modulationsverfahren
- Partitionierung des Frequenzbandes
- Leitungsankopplung durch Hybrid und Splitter
- Operation and Maintenance (OAM)

Performance-Betrachtungen
- Entwurfsziele von xDSL-Systemen
- Kanaleigenschaften von Kupferkabeln
- Charakterisierung der xDSL-Störumgebung (Nebensprechen, Funkeinkopplung und -abstrahlung, Impulsstörungen)
- spektrale Kompatibilität von xDSL-Systemen
- Interoperabilität

xDSL-Integration in übergeordnete Netzarchitekturen
- Topologie von Kupfer-Anschlussnetzen
- die Evolution im Zugangsbereich
- Ende-zu-Ende Service-Architektur
- Paketorientierte Netzarchitekturen (PPP über xDSL)
- Vorteile von ATM-Netzarchitekturen
- Beispiele: PPP over ATM, Layer 2 - Tunneling Protocol (L2TP), PPP Terminated Aggregation, PPP over Ethernet

Übersicht zur xDSL-Marktentwicklung
- kommerzielle Einführung von xDSL-Diensten weltweit
- Projektbeispiel: die ADSL-Angebote der Deutschen Telekom mit Fokussierung auf wesentliche Zielgruppen
- weitere Aktivitäten in Westeuropa
- Prognosen für die zukünftige Marktentwicklung

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung
xDSL: Technik und Nutzen des neuen Weitverkehrs-Standards

☐ Ich melde mich an zur
xDSL:Technik und Nutzen des neuen Weitverkehrs-Standards
vom 30.08. - 31.08.01 in Bonn
zum Preis von EUR 1.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Bonn

von _____ bis _____
(Übernachtung/Frühstück DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

VPN mit Windows 2000

Fortsetzung von Seite 1

Schon in Windows NT 4.0 bot sich der als kostenloses Update verfügbare Routing und RAS-Dienst als VPN-Server an, eine deutlich modernere Implementation ist jedoch seit dessen Erscheinen in Windows 2000 integriert. Dieser Umstand, verbunden mit der stetig zunehmenden Verbreitung von Windows 2000 in Firmennetzwerken sorgt für wachsende Akzeptanz und Beliebtheit der Windows 2000-VPN-Lösung – können doch auf diese Weise in einem ohnehin aus Windows 2000-Rechnern bestehenden Netzwerk u.U. nicht unerhebliche Kosten für VPN-Lösungen von Drittherstellern gespart werden.

Hierbei stellen sich jedoch einige Fragen:

- Was kann Windows 2000-VPN eigentlich? Und wie sicher ist es?
- Ist eine Firewall-orientierte VPN-Lösung nicht vorzuziehen?
- Wie sieht es mit der Interoperabilität aus?

Diese und andere Fragen versucht dieser Artikel zu beantworten.

Was kann Windows 2000-VPN?

Wie bereits angedeutet, ist in den Server-Versionen von Windows 2000 eine Reihe von Diensten integriert, die umfangreiche Routing-, RAS- und VPN-Server-Funktionalität bieten. Diese Dienste bilden administrativ eine Einheit, den sog. Routing und RAS-Service (RRAS). Zusätzlich ist in jedem Windows 2000-System bereits ein RAS- und VPN-Client enthalten.

RAS-Richtlinien

Der RAS-Server hat an Funktionsumfang deutlich zugenommen, unter anderem stehen unter Windows 2000 Remote Access Policies zur Verfügung, die eine deutlich differenziertere Steuerung der Einwahlmöglichkeiten von Usern erlauben. Remote Access Policies bestehen hierbei aus 3 Komponenten:

- Ein Set von Bedingungen (z.B. Tageszeit/ Wochentag, Gruppenmitgliedschaft usw.)
- Die aus diesen Bedingungen resultierende RAS-Berechtigung (Zugriff gestatten oder verweigern)

Der Autor

Alexander Zarenko ist seit 1996 bei der ComConsult Beratung und Planung GmbH tätig. Als Berater im Kompetenz Center Backoffice beschäftigt er sich hauptsächlich mit der Konzeption und Umsetzung von Migrationsprojekten auf Windows 2000. Schwerpunkte bilden hierbei die Themen Sicherheit, Policies & Profiles, sowie Remote Access/VPN.

- Eine Reihe von Eigenschaften, die auf die Verbindung angewendet werden (Verschlüsselungstärke, zugelassene Authentifizierungsarten usw.)

Mit diesen Mitteln lassen sich verschiedene, flexibel auf die Anforderungen abgestimmte Richtlinien erstellen. Zu beachten ist an dieser Stelle, dass ohne wenigstens eine vorhandene Richtlinie keine Einwahl möglich ist. Hierzu wird bei der Installation des Routing- und RAS-Dienstes automatisch eine Standardrichtlinie erstellt, die festlegt, dass zu jeder Zeit der Zugriff verweigert wird! Treffenderweise heißt diese Richtlinie "Zugriff erteilen, wenn Einwahlberechtigung erteilt worden ist", denn genau dies ist der Fall: beim Einwahlversuch eines Benutzers, der die Bedingungen der Richtlinie erfüllt (die ja immer erfüllt ist), überprüft der RAS-Server die Einwahleigenschaften des Benutzers. Je nachdem nimmt er hierzu seine eigene SAM (bei lokalen Usern) oder das Active Directory (bei Usern der Domäne) zur Hilfe. Wie bei NT 4.0 üblich, gibt es hier pro User den Eintrag "Zugriff gestatten" oder "Zugriff verweigern".

Hinzugekommen ist unter Windows 2000 der Punkt "Zugriff über RAS-Richtlinien steuern", der in einer einheitlichen Domäne und auf alleinstehenden Windows 2000-RAS-Servern anwählbar und dort auch die Standardeinstellung bei neu angelegten Benutzern ist. Ist beim User explizit "Zugriff gestatten" konfiguriert, überschreibt diese Einstellung die RAS-Berechtigung der Richtlinie und der Benutzer kann sich erfolgreich einwählen. Lautet die userspezifische Einstellung "Zugriff verweigern", so hat diese ebenso Vorrang vor der innerhalb der Richtlinie definierten Berechtigung. Selbst wenn in der Richtlinie "Zugriff gestatten" stünde, würde die Verbindung getrennt. Bei der Einstellung "Zugriff über RAS-Richtlinien steuern" wird schließlich die Berechtigung der Richtlinie verwendet. Somit können Administratoren RAS-Berechtigungen entweder wie bei NT 4.0 auf Benutzerbasis oder richtlinienbasiert festlegen, wobei natürlich auch Kombinationen möglich sind.

Die Zuweisung von IP-Adressen kann entweder aus einem statischen Adresspool oder per DHCP erfolgen. Bei letzterem fordert der RAS-Server 10 IP-Adressen beim DHCP-Server an und ordnet von diesen seinem (virtuellen) Einwahlinterface die erste Adresse zu. Die übrigen IP-Adressen werden beim Connect an die Clients vergeben und beim Disconnect wiederverwendet. Sind alle 10 Adressen vergeben, fordert er 10 weitere an und vergibt sie an hinzukommende Clients. Freigegeben werden die IP-Adressen erst bei Dienststop des RRAS.

Bei der Vergabe von IP-Adressen aus einem statischen Adresspool gibt es nun die Möglichkeit, Adressen aus dem selben Subnetz wie das des LAN-Interfaces des RAS/VPN-Servers zu vergeben oder ein anderes Subnetz zu wählen. Im ersten Fall sind keine weiteren Einstellungen notwendig und der Server fungiert als Proxy-Arp für seine RAS-Clients. Im zweiten Fall routet der RAS-Server zwischen seinem Einwahlinterface und der LAN-Schnittstelle und es ist erforderlich, die entsprechenden Routen auf den Intranetroutern einzutragen, damit diese den für die RAS-Clients bestimmten Verkehr auch an den RAS-Server weiterleiten - ansonsten ist nur Point-to-Point-Verkehr möglich. Falls man dies nicht manuell vornehmen möchte, kann auch RIP oder OSPF verwendet werden, unter Windows 2000 stehen beide Protokolle zur Verfügung.

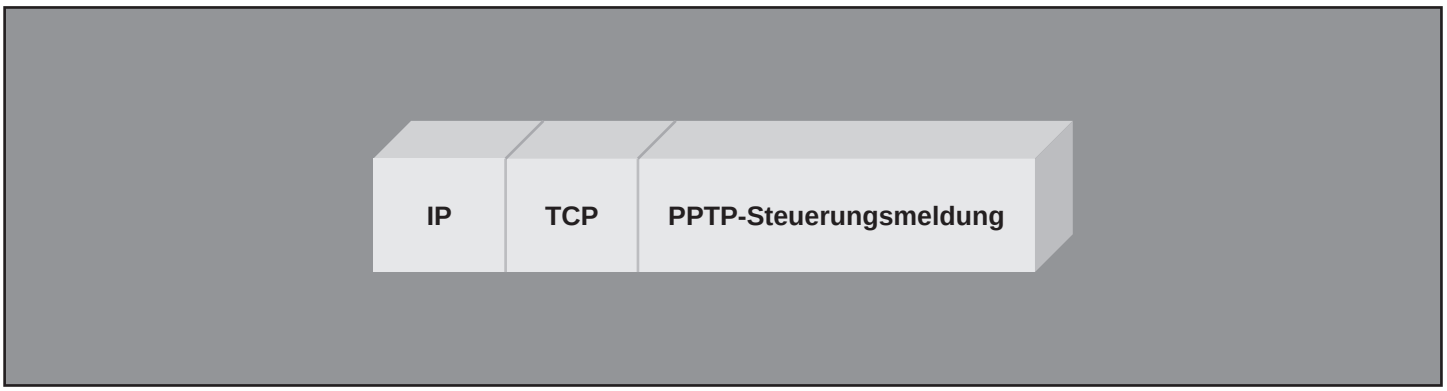


Bild 1 PPTP-Tunnelsteuerung

Was tun bei mehreren RAS-Servern?

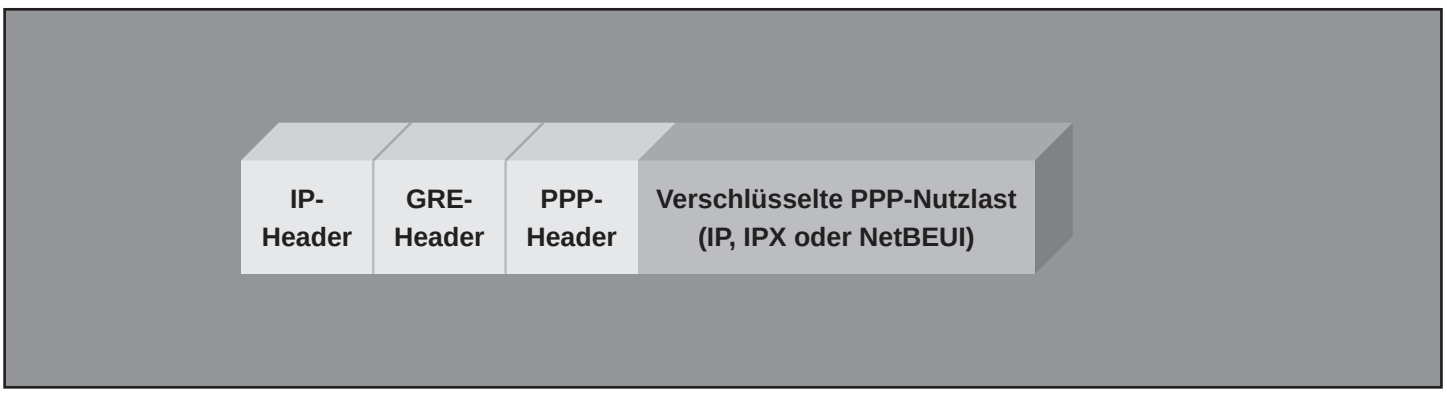
Die oben beschriebenen Remote Access Policies werden lokal auf dem RAS-Server abgelegt. Dies hat zur Folge, dass unter Umständen erheblicher Aufwand betrieben werden muss, um alle Server einheitlich zu konfigurieren, falls viele verschiedene RAS- und VPN-Server in einem Unternehmen eingesetzt werden. Abhilfe bietet hier der ebenfalls in Windows 2000 integrierte Internet Authentication Service (IAS), der die Microsoft-Implementation eines RADIUS-Servers ist. Statt alle RAS-/VPN-Server manuell einheitlich zu konfigurieren, können diese als RADIUS-Clients des IAS fungieren, wobei Authentifizierungs- und Kontoführungsaufgaben zentral vom IAS durchgeführt werden. Der IAS wiederum kann zur Überprüfung der vom RADIUS-Client gesammelten Authentifizierungdaten je nach Konfiguration auf eine Windows NT 4.0 Domäne, seine eigene SAM oder das Active Directory zugreifen. Darüber hinaus werden nicht mehr lokale, sondern zentral auf dem IAS definierte Richtlinien genutzt. Was den Umfang der verfügbaren Richtlinienoptionen oder Authentifizierungsmodi betrifft, unterscheiden sich RAS-Server und IAS nicht. Klassisches Einsatzbeispiel für den IAS ist ein "Outsourced-Dialing"-Szenario, in dem ein Unternehmen seine Einwahl-Infrastruktur an einen ISP auslagert. Authentifizierungsanfragen und Kontoführungsdaten von sich einwählenden Clients werden hierbei vom Network Access Server (NAS) des ISP an den IAS-/RADIUS-Server des Unternehmens weitergeleitet und bearbeitet. Generell ist der Einsatz des IAS jedoch überall dort sinnvoll, wo es mehr als einen RAS-Server zu verwalten gilt. Im übrigen halten sich IAS und RRAS an bestehende RFC-Standards bezüglich des RADIUS-Protokolls. Somit ist es zumindest theoretisch möglich, auch RAS-Server anderer Hersteller mit dem IAS zu nutzen, bzw. RRAS mit einem anderen RADIUS-Server als dem IAS, wobei sicherheitshalber die Interoperabilität vorher im Testumfeld überprüft werden sollte.

Tunnelprotokolle

Mit PPTP, L2TP und IPSec stehen die derzeit gängigen Tunnelprotokolle zur Verfügung.

- PPTP ist ein u.a. von Microsoft entwickeltes Layer 2 Protokoll (definiert in RFC 2637), das Benutzerauthentifizierung und Verschlüsselung bietet – jedoch keine Computerauthentifizierung. Bei PPTP werden PPP-Frames in IP-Datagramme gekapselt, um diese über ein IP-Netzwerk (z.B. Internet) zu übertragen. Die Nutzlast dieser PPP-Frames kann hierbei IP-, IPX- oder NetBEUI-Verkehr sein. Zur Tunnelerstellung, -wartung und -schließung verwendet PPTP eine getrennte TCP-Verbindung, die auch als PPTP-Steuerungsverbindung bezeichnet wird. Beim Aufbau der VPN-Verbindung erfolgt die Authentifizierung mittels derselben Authentifizierungsmechanismen wie bei PPP-Verbindungen, also beispielsweise PAP, CHAP MS-CHAP und EAP. PPTP übernimmt ebenso die Komprimierung mittels MPPC (Microsoft Point to Point Compression) und/oder Verschlüsselung der PPP-Nutzlasten von PPP mittels MPPE (Microsoft Point to Point Encryption), einer Verschlüsselungsart, die den RSA RC4-Algorithmus (nach Rivest-Shamir-Adleman) einsetzt. Bei installiertem High-Encryption-Pack können bis zu 128 Bit lange Verschlüsselungsschlüssel eingesetzt werden.

Bild 2 PPTP-getunnelte Daten



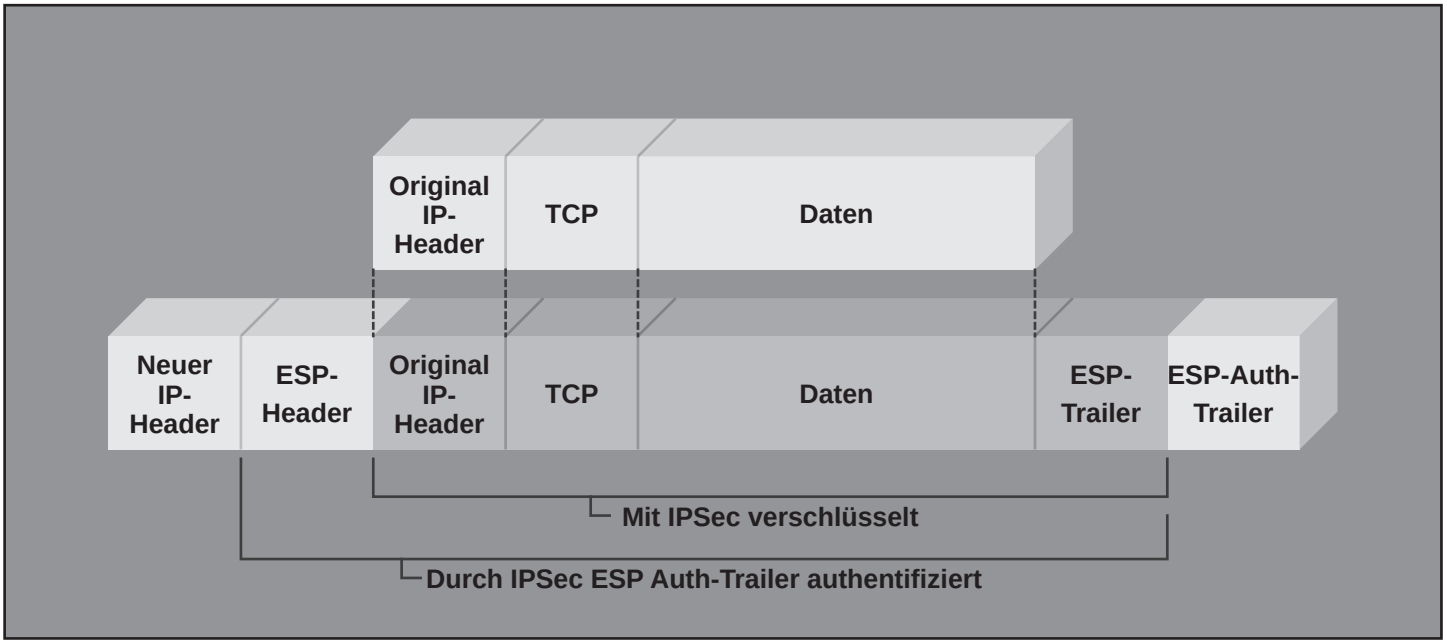
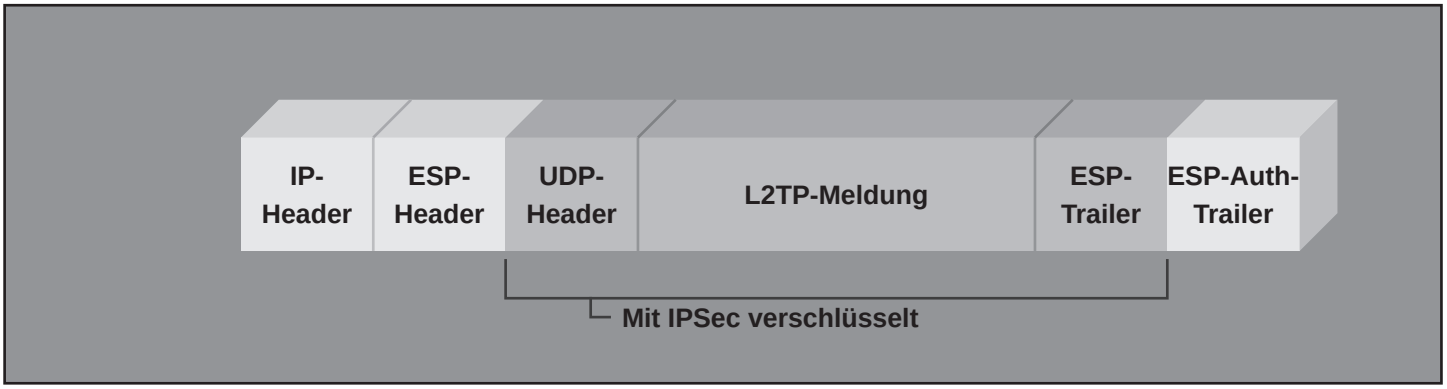


Bild 3 IPSec ESP-Tunnelmodus

- IPSec ist ein Layer 3 Protokoll, das im ESP-Tunnelmodus die Verschlüsselung und Kapselung von IP-Verkehr in einen IP-Header zur Versendung über ein IP-Netzwerk ermöglicht. Des weiteren bietet IPSec gegenseitige Computerauthentifizierung, Datenauthentifizierung und Datenintegrität. Die Computerauthentifizierung erfolgt bei Windows 2000-IPSec entweder über X.509-kompatible Zertifikate, gemeinsame Schlüssel oder im vertrauenswürdigen Domänenumfeld auch mit Kerberos v5. Für die Datenauthentifizierung und -integrität stehen die Einweg-Hashfunktionen HMAC-MD5 und -SHA1 mit bis zu 128 bzw. 160 Bit langen Hashwerten zur Verfügung. Zur Verschlüsselung nutzt IPSec die Algorithmen DES und 3DES mit 56 bzw. 168 Bit langen Schlüsseln. Diese Schlüssel werden zwischen kommunizierenden Computern über die Dienste für den Internetschlüsselaustausch (IKE) dynamisch ausgetauscht und verwaltet. Mit Windows 2000-IPSec allein ist jedoch keine Benutzerauthentifizierung möglich, weshalb der ESP-Tunnelmodus keine vollwertige VPN-Lösung für ein Client-zu-Gateway-VPN darstellt, in dem Benutzerauthentifizierung erforderlich ist.

- L2TP ist eine Kombination von L2F (Layer 2 Forwarding) und PPTP und wurde von Cisco und Microsoft entwickelt, um die Eigenschaften der beiden Tunnelprotokolle zu vereinen (definiert in RFC 2661). Es ist ebenso wie PPTP ein Layer 2 Protokoll und bietet ausschließlich Benutzerauthentifizierung. Bei L2TP werden PPP-Frames entsprechend dem Transportmedium eingekapselt. Dieses kann ein IP-, X.25-, Frame-Relay- oder ATM-Netzwerk sein. Die Nutzlast der PPP-Frames kann IP-, IPX- oder NetBEUI-Verkehr sein. Wenn über ein IP-Netzwerk gesendet wird, verwendet L2TP UDP-Meldungen sowohl für Tunnelwartung als auch getunnelte Daten (UDP-Port 1701 bei Client und Server). Beim Aufbau der VPN-Verbindung erfolgt die Authentifizierung mittels derselben Authentifizierungsmechanismen wie bei PPTP bzw. bei PPP-Verbindungen. L2TP wird in der Regel nicht einzeln eingesetzt, sondern im Verbund mit IPSec im Transportmodus. Hieraus ergibt sich eine sehr flexible und sichere Kombination.

Bild 4 L2TP-Tunnelwartung



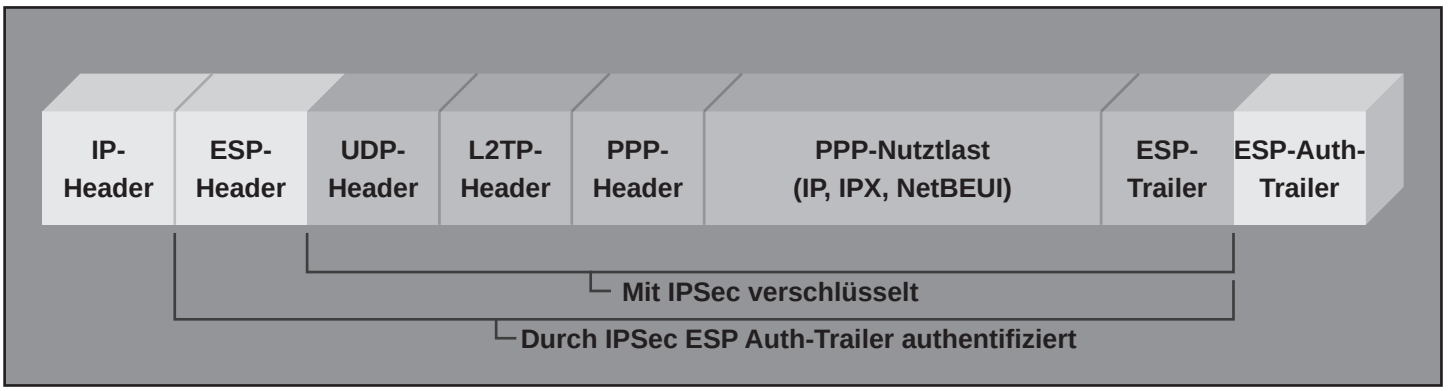


Bild 5 L2TP-getunnelte Daten

Authentifizierungsstrategien

Microsoft setzt hier klar auf die Kombination L2TP-über-IPSec als zukünftigen Defacto-Standard und wirbt sehr stark für die Nutzung bzw. Unterstützung dieser Variante durch Kunden und Hersteller von VPN-Produkten. PPTP wird hingegen für kleinere Netzwerke und Fälle, in denen NAT nötig ist, empfohlen (näheres hierzu findet sich unter Firewall vs. Windows 2000-VPN-Server). Wo auf Benutzerauthentifizierung verzichtet werden kann, könnte jedoch auch IPSec im Tunnelmodus verwendet werden, beispielsweise im Falle eines Router-zu-Router VPNs.

IPSec ist immer noch im Entwicklungsstadium und könnte in Zukunft viele der Features bieten, die momentan in PPTP und L2TP implementiert sind. Mittlerweile gibt es Bestrebungen und bereits implementierte Lösungsansätze, innerhalb des ISAKMP-Protokolls bereits existierende Mechanismen zur Benutzerauthentifizierung wie RADIUS oder SecurID zu nutzen. Einen solchen Ansatz bietet das Xauth-Verfahren. Xauth steht für "Extended Authentication" und ist in Form eines Drafts von Cisco eingereicht worden. Den Draft-Status wird das Verfahren offiziell wohl nicht verlassen, da die IPSRA- und die IPSec-Working Group einerseits keine Erweiterung von ISAKMP oder IKE akzeptieren, andererseits keine Verknüpfung von Remote Access und IPSec zulassen. Dieser Umstand hindert Cisco natürlich nicht daran, die Xauth-Unterstützung in eigene Produkte trotzdem zu integrieren, und somit wird das Verfahren letztlich auch genutzt - Standard hin oder her.

Microsoft kann somit z.Zt. zu Recht mit der Aussage werben, sich mit PPTP sowie der Kombination von L2TP und IPSec auf existierende (RFC-)Standards zu berufen, statt zu nicht standardisierten Lösungen zu greifen.

Darüber hinaus favorisiert Microsoft die Benutzerauthentifizierung mittels Smartcards auch für VPN, wobei das PPP-Authentifizierungsverfahren EAP-TLS eingesetzt wird.

Auf Smartcards und EAP-TLS wird an späterer Stelle genauer eingegangen.

Schlüsselverwaltung – die Windows 2000 PKI

Windows 2000 bietet von Hause aus die Möglichkeit, eine auf das Unternehmen und seine Bedürfnisse zugeschnittene Infrastruktur öffentlicher Schlüssel (PKI) aufzubauen.

Die Windows 2000 PKI besteht aus drei Teilen:

- Microsoft CryptoAPI und Cryptographic Service Provider (CSPs)
- Microsoft Zertifikatsdienste
- Zertifikatsspeicher

Hierbei stellt CryptoAPI eine sichere Schnittstelle für die kryptografischen Funktionen der installierbaren CSP-Module dar. CryptoAPI und CSP-Dienste stehen allen Applikationen und Diensten zur Verfügung, die kryptografische Dienste benötigen, beispielsweise muss bei der Installation der Windows 2000 Zertifikatsdienste ein CSP gewählt werden.

CSPs sind mit Modulen vergleichbar, die - wie im Fall der Smartcard CSPs - von Herstellern für die Unterstützung ihrer Hardware oder - wie im Fall der von Microsoft verfügbaren CSPs - zur Unterstützung aktueller kryptografischer Verfahren und Algorithmen bereitgestellt werden können. Unter anderem werden die folgenden CSPs mit Windows 2000 geliefert:

Microsoft Base Cryptographic Provider

Dieser CSP stammt noch aus Zeiten der US-Exportrestriktionen für kryptografische Verfahren/Schlüssellängen und ist heutzutage nicht mehr zeitgemäß. Asymmetrische Verfahren werden nur mit bis zu 1024 bit Schlüssellänge, RC2 und RC4 mit 40 bit unterstützt. Weder DES noch 3DES werden angeboten.

Microsoft Enhanced Cryptographic Provider

Hier sind alle aktuellen Standards implementiert, asymmetrische Verfahren können mit bis zu 16384 bit langen Schlüsseln arbeiten, RC2 und RC4 mit bis zu 128 bit. Darüber hinaus wird DES mit 56 sowie 3DES mit 112 und 168 Bit Schlüssellänge unterstützt.

Smart Card Cryptographic Service Provider

Zwei verschiedene CSPs für Smartcards ermöglichen die Unterstützung für Gem-SAFE- und Cryptoflex-Smartcards der Firmen Gemplus und Schlumberger.

Die Microsoft Zertifikatsdienste sind in den Windows 2000-Serverversionen enthalten und bilden den Kern einer Windows 2000 PKI. Ihre Aufgaben sind die Vergabe und das Management von Zertifikaten nach dem X.509-Standard. Zertifikate dieses Typs werden von einer Vielzahl von Produkten auch anderer Hersteller unterstützt, da es sich um die aktuelle Standard-Zertifikatsform handelt.

Die Zertifikatsdienste unter Windows 2000 unterstützen ein hierarchisches CA-Modell mit Stammzertifizierungsstellen (Root-CA), Zwischenzertifizierungsstellen (PCA) und ausstellenden Zertifizierungsstellen (CA).

Darüber hinaus werden auch externe CAs – wie z.B. solche anderer Unternehmen oder kommerzieller Serviceprovider – unterstützt.

Wird unter Windows 2000 eine sogenannte Organisationszertifizierungsstelle eingerichtet, so ist diese automatisch mit dem Active Directory gekoppelt. Active Directory enthält für die Organisationszertifizierungsstelle relevante Informationen wie Namen der Benutzerkonten, Zugehörigkeiten zu Sicherheitsgruppen und ein Set von Zertifikatsvorlagen, u.a. für IPSec-Authentifizierung und Smartcard-Anmeldung. Sämtliche Organisationszertifizierungsstellen werden automatisch im Active Directory erfasst. Von ihnen ausgegebene Zertifikate werden an das Active Directory oder an die Computer des Anforderungssenders übermittelt. Darüber hinaus veröffentlichen sie die Zertifikatssperrlisten (Certificate Revocation Lists, kurz CRL) ebenfalls im Active Directory oder alternativ auf Webseiten oder öffentlichen Ordnern, so dass diese Informationen automatisch von jedem Punkt innerhalb der Organisation abrufbar sind. Außerdem ist es möglich, per Gruppenrichtlinien (definiert in und verteilt durch das Active Directory) automatisch Zertifikate an Windows 2000-Computer, -Benutzer und -Dienste zu verteilen.

Active Directory folgt eingeschränkt dem X.500-Standard, LDAP ist das Standardzugriffsverfahren.

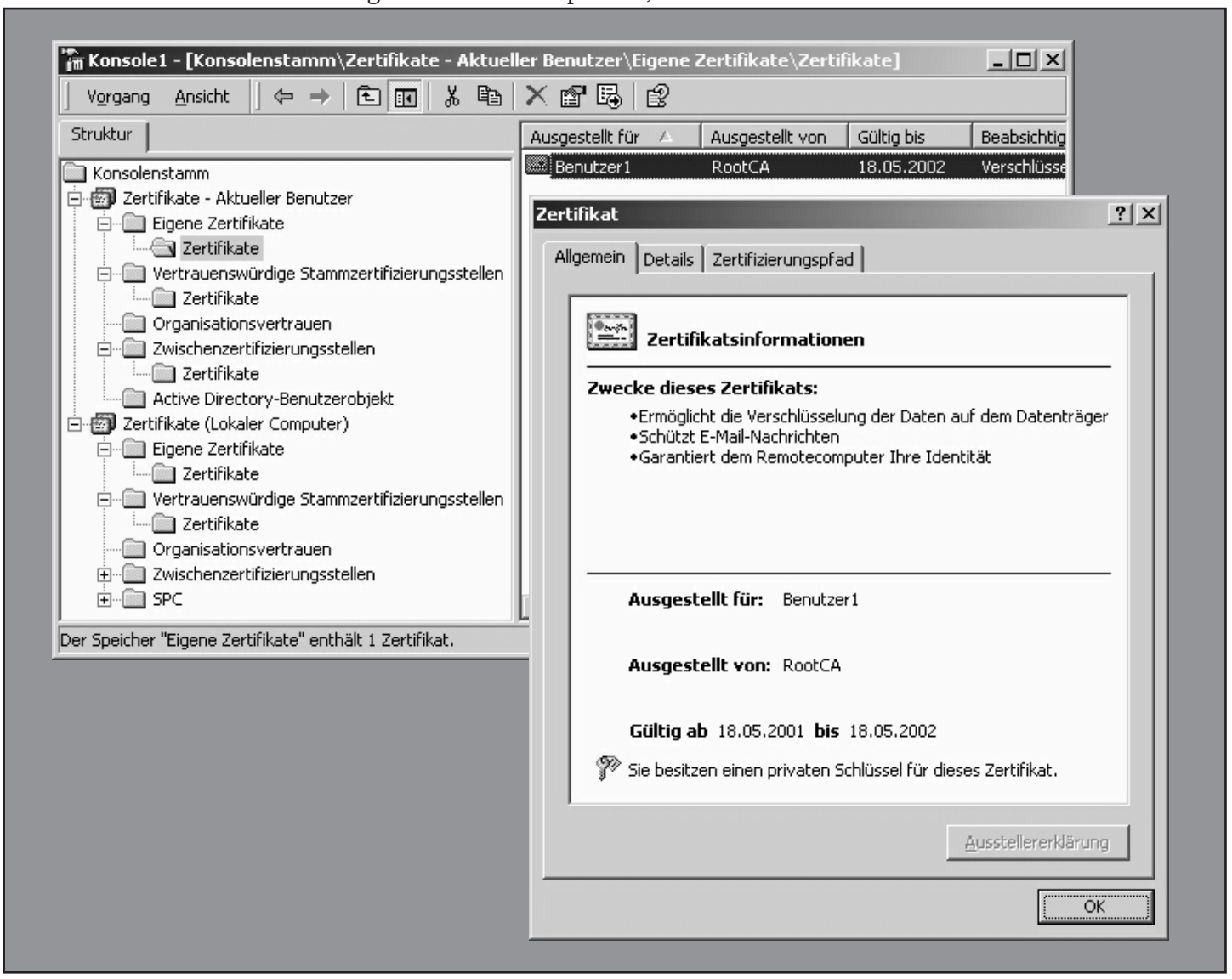
Objekte wie Zertifikate und CRLs werden in Zertifikatsspeichern abgelegt, damit User, Dienste und Computer auf sie zugreifen können.

Hierbei unterscheidet man zwei verschiedene Arten von Speichern:

Physikalische Zertifikatsspeicher

Physikalische Zertifikatsspeicher bezeichnen den Ort, an dem die Objekte tatsächlich physikalisch abgespeichert werden. Dies kann die Registry oder das Active Directory sein. Durch die Benutzung logischer Zertifikatsspeicher wird der gemeinsame Zugriff von vielen Usern, Diensten und Computern auf diese physikalischen Speicherbereiche ermöglicht, ähnlich der Funktion eines Zeigers oder einer Verknüpfung mit einer Datei.

Bild 6 Logische Zertifikatsspeicher, Benutzerzertifikat



VPN mit Windows 2000

Logische Zertifikatsspeicher

Logische Zertifikatsspeicher stellen organisatorische Bereiche bereit (z.B. "Eigene Zertifikate" eines Users oder "Vertrauenswürdige Stammzertifizierungsstellen"). In diesen Bereichen enthaltene Objekte zeigen auf deren physikalischen Speicherort. Betrachtet man beispielsweise einen Rechner mit mehreren Benutzern, so zeigt etwa ein Zertifikat, das in "Vertrauenswürdige Stammzertifizierungsstellen" eines Users abgelegt ist, unter Umständen auf den gleichen physikalischen Ort wie das eines anderen Users. So können unnötige Duplikate vermieden werden und man braucht sich um den tatsächlichen Speicherort des Zertifikats nicht zu kümmern.

Wo liegen die privaten Schlüssel?

An Endbenutzer ausgegebene Zertifikate und private Schlüssel werden an einem gesicherten Ort aufbewahrt, der sich entweder auf dem lokalen System oder auf einer Smartcard befindet. Smartcards bieten hier einen hardwareseitigen Schutz. So enden Versuche, Schlüssel auszulesen oder auch mechanische Manipulationen mit einer unbrauchbaren Karte. Auf einem üblichen Windows 2000-System besteht ein solcher Hardwareschutz natürlich nicht. Zertifikate und Private Keys werden hier im userbezogenen Teil der Registry eines Rechners abgelegt - also in der ntuser.dat, die sich im Benutzerprofil befindet. Dieser Bereich wird auch als Protected Store bezeichnet. Sollen Zertifikate und Schlüssel eines Users auch auf anderen Rechnern zur Verfügung stehen, müssen entweder servergespeicherte Profile eingesetzt werden, oder ein relativ umständlicher und sicherheitstechnisch bedenklicher Export durchgeführt werden, beispielsweise in Dateiform auf Diskette mit anschließendem Import auf dem Zielrechner.

Jedes Objekt innerhalb des Protected Store wird einzeln mit seinem eigenen Schlüssel verschlüsselt, wobei der Schlüssel sich vom Passwort des Benutzers ableitet. In nordamerikanischen Versionen von Beginn an, bei uns erst seit Lockerung der Exportrestriktionen, wird hierzu das 3DES-Verfahren mit 168 Bit langem Schlüssel verwendet. Hier gab es in der Vergangenheit einen Bug, der aber seit einiger Zeit behoben ist: Trotz installiertem High-Encryption-Pack wurde weiterhin nur schwach verschlüsselt (40 Bit), was eine enorme Sicherheitslücke darstellte. Ein kurz nach Entdeckung des Bugs herausgegebener Hotfix, der übrigens im später erschienenen Service Pack 1 für Windows 2000 enthalten ist, korrigierte diesen Fehler.

Windows 2000 und Smartcards

Smartcards sind sozusagen "Mini-Computer", die in eine flache Plastikkarte eingebettet sind. Abgesehen vom fehlenden Magnetstreifen sehen sie genauso aus wie übliche EC- oder Kreditkarten, mit dem Unterschied, dass sie wesentlich mehr Daten aufnehmen können (z.B. 8 K bei GemSAFE-Smartcards). Windows 2000 unterstützt das ICC-Format (Integrated circuit cards) - Karten dieses Typs sind in der Lage, komplexe Operationen wie digitale RSA-Signaturen durchzuführen. Statt sich nun wie üblich mit einem Benutzernamen und Passwort anzumelden, schiebt der User seine Smartcard in den an seinen Computer angeschlossenen Smartcard-Reader und gibt seine zur Smartcard passende PIN ein - ganz wie am Geldautomat der Bank. Von den beiden existierenden IC-Smartcard-Typen - denen mit Kontakten und den kontaktlosen - werden erstere von Windows 2000 unterstützt. Sie zeichnen sich durch eine goldene Kontaktplatte auf der Oberseite aus, ähnlich dem Geldkartenchip auf neueren EC-Karten. Die enthaltenen 8 Kontakte stellen die Verbindung zwischen dem eingebetteten Chip und dem Smartcard-Reader her.

Im Lieferumfang von Windows 2000 sind zwei verschiedene CSPs (Cryptographic Service Provider) enthalten, die von den jeweiligen Herstellern von Smartcards zur Unterstützung ihrer Produkte für Windows 2000 entwickelt wurden. Gemplus steuerte hierzu den CSP für GemSAFE-, Schlumberger den CSP für Cryptoflex-Smartcards bei. Weitere RSA-basierte Smartcards werden von Windows 2000 ebenso unterstützt, sofern deren Hersteller einen CSP für Windows 2000 zur Verfügung stellen. Darüber hinaus sind für einige gängige Smartcard-Reader die notwendigen Treiber bereits in Windows 2000 integriert, beispielsweise für Gemplus- und Schlumberger-Reader mit seriellem Port, USB- und PCMCIA-Varianten sind aber ebenso verfügbar.

Lokale Authentifizierung in Windows 2000

Als Standardauthentifizierungsprotokoll in Windows 2000 wird Kerberos v5 eingesetzt. Bei der interaktiven, lokalen Anmeldung mit Smartcards wird eine im Kerberos-Protokoll definierte Erweiterung genutzt, die innerhalb von Kerberos den Einsatz von Zertifikaten zur Authentifizierung ermöglicht. Auf einige Detailelemente wird in der folgenden Ablaufbeschreibung bewusst verzichtet, es soll lediglich ein Überblick über die generelle Funktionsweise gegeben werden.

Authentifizierung mit Benutzername und Passwort:

1. Benutzer meldet sich an, Kerberos-Client generiert eine Authentifizierungsanfrage. Diese verschlüsselt er standardmäßig mittels RC-4, wobei der aus seinem (eingetippten) Passwort gebildete MD-4-Hashwert als Schlüssel verwendet wird. In der Anfrage bekundet der Client die Absicht, mit dem Ticket Granting Service (TGS) in Verbindung treten zu wollen, um ein Ticket Granting Ticket (TGT) zu erhalten.

2. Jeder Windows 2000 Domänencontroller ist gleichzeitig auch Key Distribution Center (KDC). Auf dem KDC laufen zwei verschiedene Kerberos-Dienste, der Authentication Service (AS) und der schon erwähnte TGS. Die Authentifizierungsanfrage wird an den AS des KDC geschickt.

3. Hat der Benutzer das richtige Passwort eingegeben, ist es dem KDC möglich, mit dem ihm zur Verfügung stehenden Paßworthash die Authentifizierungsanfrage des Clients zu entschlüsseln. Anschließend entnimmt er einen Teil der entschlüsselten Anfrage, verschlüsselt diese kürzere Version erneut mit dem Paßworthash und schickt sie an den Client zurück. In dieser Meldung ist zusätzlich das spezielle Session Ticket enthalten, das für die Verbindung zum TGS notwendig ist, das sog. Ticket Granting Ticket (TGT). Session Tickets werden mit einem vom KDC generierten Schlüssel verschlüsselt, den nur er selbst und die angefragte Zielressource kennen. In diesem Fall ist der KDC selbst die Zielressource und damit auch der einzige, der diesen Schlüssel kennt. Der mit dem Paßworthash des Users verschlüsselte Session Key ist ebenso in der Meldung enthalten.

4. Der Client entschlüsselt den für ihn verschlüsselten Session Key und legt das ebenfalls erhaltene Ticket in seinem Ticketspeicher ab.

5. Der Client generiert eine TGS-Anfragemeldung, die unter anderem das erhaltene TGT (dieses Ticket autorisiert ihn als Anfragenden) und die Angabe der Zielressource, auf die der Client zugreifen will, enthält.

6. Der KDC stellt ein Session-Ticket für die angefragte Zielressource aus.

Authentifizierung mit Smartcard

Bei der Anmeldung mit Smartcards gibt es nun bei den Punkten 1, 3 und 4 einige wichtige Unterschiede:

- In der Authentifizierungsanfrage (Punkt 1) sendet der Client statt der verschlüsselten Zeichenkette das von der Smartcard extrahierte Zertifikat.
- Der KDC überprüft die Gültigkeit des Zertifikats und benutzt den im Zertifikat enthaltenen öffentlichen Schlüssel des Users zur Verschlüsselung des Session Key. In seiner Antwortmeldung an den Client sendet der Server das verschlüsselte TGT und den mit dem öffentlichen Schlüssel des Users verschlüsselten Session Key (Punkt 3).
- Der Client bzw. der User ist der einzige, der diesen Session Key entschlüsseln kann, da nur er im Besitz seines privaten Schlüssels ist. Dieser ist, wie bereits erwähnt, auf der Smartcard gespeichert. Somit kommt er, wie auch im vorigen Beispiel, an den entschlüsselten Session Key (Punkt 4) und kann weitere Schritte einleiten (Punkt 5).

Das Kerberos-Authentifizierungsprotokoll kommt jedoch nicht bei der Authentifizierung im Zusammenhang mit RAS bzw. VPN zum Einsatz - der Grundgedanke ist jedoch ähnlich.

Remote-Authentifizierung mit Smartcards

Wie schon beschrieben wird hier das Verfahren EAP-TLS genutzt. EAP ist eine PPP-Erweiterung, über die beliebige Authentifizierungsmechanismen für die Gültigkeitsprüfung einer PPP-Verbindung verwendet werden können. Zu Beginn der Authentifizierungsphase handeln die PPP-Peers aus, welches EAP-Authentifizierungsschema (der sog. EAP-Typ) verwendet werden soll. Die EAP-Architektur ist modular ausgelegt und ermöglicht so, dass durch die Installation einer EAP-Bibliothekdatei auf dem RAS-Client und dem RAS-Server jederzeit neue Authentifizierungsschemata bereitgestellt werden können. Ein Beispiel hierfür ist der von der Firma RSA Security angebotene RSA ACE/Agent for Windows 2000, in dem u.a. eine solche Bibliothekdatei enthalten ist. Hiermit wird die Interoperabilität zwischen dem RSA-eigenen Token-basierten Authentifizierungsmechanismus und dem Windows 2000 RAS-/VPN-Server ermöglicht.

Der mit Windows 2000 mitgelieferte EAP-Typ EAP-TLS ist eine Implementation des Transport Layer Security-Protokolls innerhalb des EAP-Gerüsts. Allgemein betrachtet bezeichnet EAP-TLS einen starken Authentifizierungsmechanismus, bei dem die gegenseitige Authentifizierung von PPP-Client und authentifizierendem Computer durch Austausch und Überprüfung von Zertifikaten durchgeführt wird. Hierbei sendet der RAS- oder IAS-Server sein Computerzertifikat und der Client sein von der Smartcard des Users extrahiertes Zertifikat zur Smartcardanmeldung. Teile der Kommunikation werden mit dem jeweiligen privaten Schlüssel digital signiert. Nach abgeschlossener erfolgreicher Validierung der übermittelten Zertifikate wird die digitale Signatur des Kommunikationspartners auf beiden Seiten mit dem im Zertifikat enthaltenen öffentlichen Schlüssel überprüft.
Unter Windows 2000 wird EAP-TLS nur von RAS-Servercomputern unterstützt, die Teil einer gemischten oder einheitlichen Domäne sind, d.h. nicht von alleinstehenden Servern. Dies ist leicht nachzuvollziehen, wenn man z.B. bedenkt, dass Smartcards nur im Zusammenhang mit Organisationszertifizierungsstellen herausgegeben werden können und zur Zuordnung von Zertifikaten zu Usern der Zugriff auf das Active Directory benötigt wird.

Smartcard Roll-out

Das Roll-out von Smartcards stellt sicherheitstechnisch eine sehr brisante Angelegenheit dar. Da es weder praktikabel noch sinnvoll ist, diesen Vorgang in die Hände des jeweiligen Users zu legen, fällt diese Aufgabe Administratoren zu, die dadurch in den Besitz des privaten Schlüssels des Users kommen und somit - zumindest digital - seine Identität annehmen können. Dies ist generell nicht zu vermeiden, da es notwendig ist, dass ein Administrator Zertifikate im Namen anderer Benutzer anfordert und diese inklusive des privaten Schlüssels auf der Smartcard ablegt. Zu diesem Zweck gibt es ein spezielles Zertifikat, das sogenannte Registrierungsagentzertifikat, auch Administratorsignaturzertifikat genannt. Mit dem zum Zertifikat gehörenden privaten Schlüssel müssen alle diesbezüglichen Anforderungen digital signiert werden, so dass der Besitz des privaten Schlüssels des Registrierungsagenten zwingende Voraussetzung für solche Anforderungen ist. In der Regel wird das Registrierungsagentzertifikat an einen nur zu diesem Zweck eingerichteten Benutzer ausgegeben, der fortan für sämtliche Zertifikatsanforderungen im Zusammenhang mit Smartcards verwendet wird.

Für die Anmeldung mit Smartcards stehen zwei verschiedene Zertifikatsvorlagen zur Verfügung: Smartcard-Anmeldung erlaubt, wie der Name schon sagt, die Anmeldung mit Smartcards, Smartcard-User erlaubt zusätzlich die digitale Signatur und Verschlüsselung von E-Mail.

Zusammenfassung

Zusammenfassend lässt sich feststellen, dass die Windows 2000-Authentifizierung mit Smartcards eine sehr sichere Angelegenheit ist - allein schon wegen der notwendigen Kombination aus Besitz (der Smartcard) und Wissen (Kenntnis der PIN). Kryptografische Operationen werden von der Smartcard selbst durchgeführt, wobei der private Schlüssel stets auf ihr verbleibt - er wird in keiner Form während der Authentifizierung übertragen. Des weiteren werden häufige Kennwortänderungen überflüssig und Benutzer müssen sich anstelle eines langen und kryptischen Passworts lediglich ihre PIN merken. Derzeit aktuelle Smartcards wie z.B. GemSAFE von Gemplus sind sogar nach 3-maliger Fehleingabe der PIN in Folge elektrisch unbrauchbar und können daraufhin nicht wiederverwendet werden. Eine entsprechende Sensibilisierung der Benutzer hinsichtlich dieses Umstands vorausgesetzt, bedeutet dies eine konsequente und sinnvolle Sicherheitsmaßnahme, die Brute-Force-Attacken bei Verlust der Smartcard nahezu unmöglich macht.

Firewall vs. Windows 2000-VPN-Server

Die meisten modernen Firewalls bieten zusätzlich zu ihren sonstigen Sicherheitsfeatures VPN-Server- bzw. VPN-Gateway-Funktionalität und stellen für verschiedene Betriebssysteme den dazu passenden VPN-Client zur Verfügung. Die Tatsache, dass VPN-Gateway und Firewall sich auf ein und derselben Maschine befinden, versetzt die Firewall in die Lage, auch die über das VPN gesendeten Pakete überprüfen zu können. Dies ist dadurch bedingt, dass die Firewall als ein Tunnelendpunkt ebenfalls die Ver- und Entschlüsselung vornimmt.

Bei der Frage nach der Positionierung eines Windows 2000-VPN-Servers scheiden sich die Geister – aus Sicherheitsgründen sollte jedoch ein Platz hinter der Firewall gewählt werden, zur Minimierung des Schadens im Falle eines erfolgreichen Angriffs möglichst in einer eigens für VPN-Server eingerichteten DMZ.

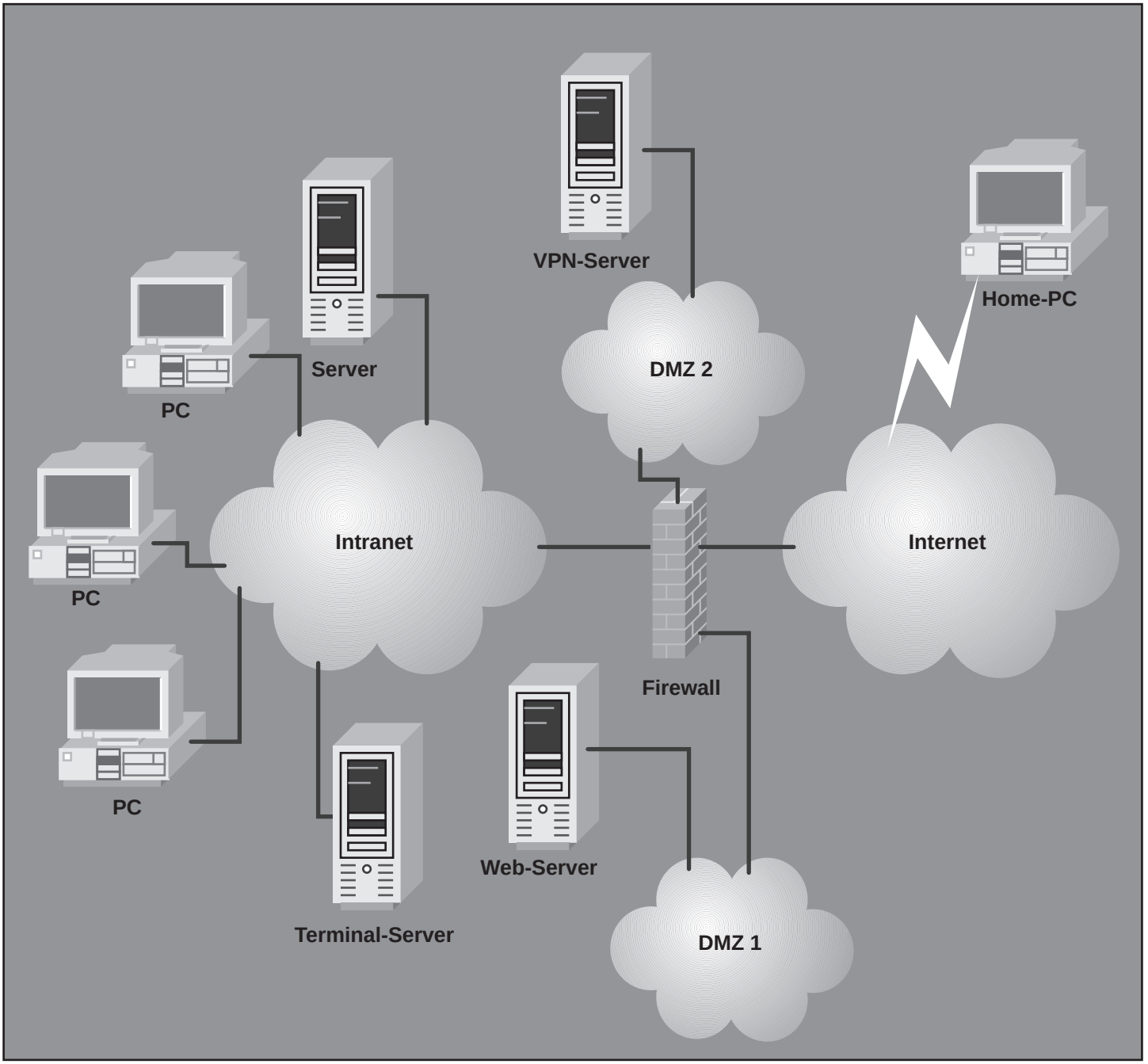


Bild 7 VPN-Server in eigener DMZ mit VPN-Client im Internet

Steht der VPN-Server hinter der Firewall, verhindert dies die Überprüfung des Inhalts der über den VPN-Tunnel gesendeten Pakete, sofern diese verschlüsselt sind, da der Tunnel nicht an der Firewall, sondern am dahinterliegenden VPN-Server terminiert wird. Obwohl es so erscheint, ist dies tatsächlich kein Nachteil - vorausgesetzt, es werden ausreichende Sicherheitsmaßnahmen ergriffen, um den Zugang zu den Tunnelendpunkten zu kontrollieren.

Bei Nutzung von L2TP-über-IPSec können hierzu beispielsweise Computerzertifikate zur Rechnerauthentifizierung sowie Smartcards als Form der starken Benutzerauthentifizierung verwendet werden. Steht der VPN-Server in einer DMZ, so kann darüber hinaus das (dann unverschlüsselte) Verkehrsaufkommen zwischen der DMZ und dem Intranet durch die Firewall überprüft werden.

NAT stellt ein Ausschlusskriterium für L2TP-über-IPSec dar, da IKE-Aushandlungen, die den ersten Schritt einer solchen Verbindung ausmachen, nicht mit NAT übersetzt werden können. Sollten keine öffentlichen Adressen für VPN-Zwecke zur Verfügung stehen oder sonstige Gründe die Verwendung privater IP-Adressen in der DMZ des VPN-Servers vorschreiben, so bleiben 3 Alternativen:

- PPTP mit MPPE als Tunnelprotokoll einsetzen,
- auf die Windows 2000-Lösung verzichten und die NAT betreibende Firewall als VPN-Gateway nutzen,
- die Firewall durch ein Windows 2000-basiertes System mit Firewall-Funktionalität ersetzen (z.B. Microsoft ISA-Server). Eine Bewertung des MS-ISA-Servers ist jedoch nicht Gegenstand dieses Artikels.

Fällt die Entscheidung auf PPTP und MPPE, gewinnt die Absicherung des Clients aufgrund der ohne IPSec nicht möglichen Computerauthentifizierung noch mehr an Bedeutung.

Streng genommen muss man VPN-Client und -Server als gleichwertige Partner betrachten, die beide im gleichen Maße vor Angriffen geschützt werden müssen. In der Praxis ist dies meist nicht vollständig umsetzbar, Ansätze hierzu sind jedoch in Produkten wie Raptor Mobile von Symantec/Axent oder dem VPN-1 Secure Client von Checkpoint implementiert, in denen zu diesem Zweck sogar eine "Personal Firewall" integriert ist, die auf dem Client-PC installiert wird.

Derart umfangreiche Sicherheit ist unter Windows 2000 mit Bordmitteln nur annähernd erreichbar – mittels Paketfilter, konsequenter Dienstereduzierung auf das absolut notwendige und den schon genannten Authentifizierungsmechanismen (Zertifikate, Smartcards) lässt sich aber ein vernünftiges Sicherheitsniveau erzielen.

Darüber hinaus kann natürlich ein Personal-Firewall-Produkt eines Drittherstellers zusätzlich installiert werden.

Generell empfiehlt sich der Einsatz eines dedizierten PCs für den VPN-Zugriff, egal welche VPN-Lösung gewählt wird, wobei klar ist, dass dies nicht in allen Fällen realisierbar ist. Ausreichender Schutz vor Viren und Trojanern mit Drittprodukten sollte darüber hinaus selbstverständlich sein.

Grundsätzlich gilt auch hier die alte Regel, dass ein System nur so sicher ist, wie sein schwächstes Glied – welches in diesem Fall der Client darstellt.

Hier sind konsequente Umsetzung eventuell auch unpopulärer Sicherheitsmaßnahmen und die Sensibilisierung der Benutzer gefragt, um ein für alle Seiten akzeptables Verhältnis zwischen Sicherheit und Bedienkomfort zu erzielen.

Fazit

Werden die nötigen Voraussetzungen geschaffen, ist eine VPN-Lösung mit Windows 2000 sehr sicher - dies gilt natürlich nur, falls in Zukunft keine gravierenden Sicherheitslöcher in Windows 2000 publik werden, von denen heute niemand etwas ahnt.

Interoperabilität

Aufgrund der großen Anzahl verschiedener Produkte werden an dieser Stelle exemplarisch zwei bedeutende Hersteller von VPN- und Firewallprodukten herausgegriffen. Leider sind die Angaben der Hersteller zu diesem Thema relativ spärlich gesät, es lassen sich aber Tendenzen erkennen.

- Cisco und Microsoft sprechen von einer strategischen Allianz, deren Ziel u.a. die Gewährleistung der Interoperabilität ihrer Produkte ist. Ob einzelne Cisco-Produkte mit dem VPN-Client und den Zertifikatsdiensten von Microsoft zusammenarbeiten können, ist im Einzelfall zu prüfen - die Tatsache, dass L2TP auch von Cisco entwickelt wurde, legt jedoch nahe, dass der VPN-Client von Windows 2000 mit den meisten Cisco-Produkten kooperieren sollte. Herstelleraussagen zufolge ist dies zumindest für die Cisco VPN 3000 Concentrator Serie gewährleistet, die auch mit den Zertifikatsdiensten zurecht kommt. Letzteres gilt laut Cisco auch für die Cisco PIX Firewall sowie den Cisco Secure VPN Client 1.1.
- Checkpoint arbeitet laut eigener Aussage in dieser Hinsicht ebenfalls intensiv mit Microsoft zusammen. Einer offiziellen Pressemitteilung zufolge hat Checkpoint angekündigt, die erweiterten Fähigkeiten der Windows 2000-Plattform nutzen und fest in seine Produktpalette integrieren zu wollen. Insbesondere wurden an dieser Stelle Microsoft-Schlüsseltechnologien wie Active Directory, die Windows 2000-Zertifikatsdienste sowie der L2TP-/IPSec-Client genannt. Hierbei ist jedoch anzumerken, dass es bisher bei Ankündigungen geblieben ist. Checkpoint hat lediglich seine bisherige Produktpolitik fortgesetzt und einen VPN-1 SecuRemote bzw. Secure Client für Windows 2000 veröffentlicht.

Zusammenfassend ist festzustellen, dass diese beiden Hersteller mit hohem Marktanteil die Kompatibilität ihrer Produkte mit der Windows 2000 VPN- und PKI-Lösung entweder bereits implementiert oder zumindest für zukünftige Versionen eingeplant haben.

Dieser Umstand wird in Verbindung mit der hohen Marktdurchdringung von Microsoft höchstwahrscheinlich zu einer hohen Akzeptanz der Windows 2000 Zertifikatsdienste und des Windows 2000 VPN-Clients/-Servers bei den Kunden führen.

Dies wiederum zieht erfahrungsgemäß ein verstärktes Interesse weiterer Drittanbieter nach sich, ihre Produkte mit den Windows 2000-Lösungen kompatibel zu machen.

Fazit
VPN mit Windows 2000?

Gerne!

Wenn die nötigen Voraussetzungen geschaffen werden oder bereits geschaffen sind, steht dem nichts entgegen.

Windows 2000 bietet bis auf wenige Ausnahmen alle relevanten Features, die eine vollwertige VPN-Lösung ausmachen, von denen viele hier nur ansatzweise vorgestellt wurden.

Behalten manche anderen Hersteller ihre bisherigen Preise bei, so kann der Einsatz einer Windows 2000-VPN-Lösung in einem ohnehin bestehenden oder geplanten Windows 2000-Netzwerk eine kostengünstige Alternative darstellen.

Seinen besonderen Reiz erhält die Windows 2000-Lösung vor allem durch die Nutzung der optionalen Komponenten, die entweder direkt oder indirekt mit dem Thema VPN in Verbindung stehen. So kann eine Komplettlösung mit Active Directory, PKI, RAS/VPN, IAS und Smartcards geschaffen werden, die weit über eine bloße VPN-Lösung hinausgeht und sich nahtlos in ein bestehendes Windows 2000-basiertes Netzwerk eingliedert.

Der neue ISA-Server könnte darüber hinaus auch die letzten Lücken schließen, wenn er hält, was er verspricht.

Sollte mit dem zusätzlichen Einsatz des ISA-Servers auch die letzte Sicherheits-Bastion zugunsten von Microsoft-Produkten gefallen sein, ist jedoch Vorsicht angeraten.

Nicht dass Sicherheitslösungen anderer Hersteller von Beginn an frei von Bugs sind – die komplette Netzwerksicherheit des Unternehmens in die Hände eines Herstellers zu legen ist generell nicht ungefährlich – kleinste Fehler im System können dann u.U. schnell großen Schaden anrichten.

ComConsult Certified Network Engineer

"...wenn die Grundlagen fehlen, dann hat man Probleme."

Jürgen Reiß (35) arbeitet bei der Rexel Region Mitte als Vertriebsmitarbeiter für Datennetzwerkkomponenten für Elektriker und Systemhäuser. der Netzwerk Insider sprach mit ihm unmittelbar nach seiner erfolgreichen Prüfung zum ComConsult Certified Network Engineer.

Insider: Von Conectis hatten wir schon einige Ihrer Kollegen hier. Kommen Sie auch aus Hannover?

Jürgen Reiß: Nein, ich komme aus Nürnberg.

Insider: Was sind Ihre Aufgaben bei Rexel?

Jürgen Reiß: Ich bin im Innendienst und zuständig für die Region Nordbayern. Ich bin zuständig für die Planung und alles, was halt zum Vertrieb dazugehört: Lieferzeiten abklären, Angebote erstellen, Leistungsverzeichnisse ausführen usw.

Insider: Welche Ausbildung haben Sie?

Jürgen Reiß: Elektrogroßhandelskaufmann. Ich bin bei der Firma bzw. der Vorgängerfirma jetzt mittlerweile 20 Jahre.

Insider: Wie geht das, wenn Sie doch erst 35 jahre alt sind?

Jürgen Reiß: Ich habe dort gelernt. Mittlerweile gehöre ich da zum Inventar (lacht).

Insider: Es ist ja von Ihrem Aufgabenbereich etwas ungewöhnlich, dass Sie den CCNE machen. Wie kamen Sie denn dazu?

Jürgen Reiß: Im Endeffekt nur dadurch, dass ein Kollege, der das Aufgabengebiet vorher gemacht hat, gekündigt hat. Der war zu dieser Ausbildung anmeldet und als er aufhörte, hat man mich dann eben dahingeschickt.

Insider: Da waren sie also quasi die Vertretung?

Jürgen Reiß: Ja. Aber ich habe das vorher schon so teilweise mitbearbeitet. Teilweise Installationsmaterial, teilweise Netzwerkartikel. Aber ich fand das schon sehr gut. Und heute bin ich nur noch für den Netzwerkvertrieb zuständig.

Insider: Was haben Ihnen die Kurse gebracht?

Jürgen Reiß erhält sein Zertifikat von Dr. Jürgen Suppan (rechts unten)

Jürgen Reiß: Wichtig war für mich, dass ich das von Grund auf lerne, denn wenn die Grundlagen fehlen, dann hat man Probleme.

Insider: Und wie haben Ihnen die Kurse gefallen?

Jürgen Reiß: Nach dem Grundlagenkurs habe ich TCP/IP gemacht, dann Internetworking und zum Schluss Ethernet-Technologien. Ich habe für die Kurse ungefähr ein halbes Jahr gebraucht. Der Grundlagenkurs (Lokale Netze) ist ein Kurs für sich. Der hat eine Qualität, die ist von keinem anderen erreicht worden. TCP/IP rangiert für mich ganz hinten. Das lag an dem Referenten*, den wir damals hatten.

* in diesem TCP/IP-Seminar hatte ein neuer Referent seine "Feuerprobe". Die Kritik ist berechtigt, und auf Veranlassung von Dr. Jürgen Suppan wurde der Referent am 2. Tag ausgetauscht.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Design Windows 2000 Active Directory, 18. - 20.06.01 im Holiday Inn Bonn

Das Seminar vermittelt, unterstützt durch den Praxisbezug zu Projekten in diesem Umfeld, wie das Active Directory zu strukturieren ist und legt dabei großen Wert auf den Entwurf der strategischen Komponenten (Domäne, Standort).
Referenten: Markus Holländer, Michael van Laak, Frank Neunzig, ComConsult Beratung und Planung Preis: EUR 1.590,--

Prozess-Optimierung, 18. - 19.06.01 im Holiday Inn Bonn

In diesem Seminar lernen Führungskräfte und Spezialisten die methodischen Grundlagen der Wege zur Optimierung von Geschäftsprozessen um Verbesserungen in unternehmensinternen Strukturen und Abläufen zu realisieren.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.290,--

Windows 2000 – Die richtige Entscheidung? 18. - 20.06.01 im Holiday Inn Bonn

Das Seminar befasst sich mit der neuen Generation des Microsoft Multitasking Betriebsystem Windows NT 4.0, das server- wie clientseitig weltweit etabliert ist: Windows 2000 mit BackOffice 2000, SQL Server 2000 und Exchange Server 2000.
Referent: Dipl.-Ing./MCSE Martin Barbian, ITC GmbH Preis: EUR 1.590,--

Zusatztermin: Lokale Netze für Einsteiger, 18. - 22.06.01 in der AGIT Aachen

Das Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Roland Moos, Dr. Jürgen Suppan Preis: EUR 1.990,--

Projekt-Management-Workshop, 21. - 22.06.01 im Holiday Inn Bonn

Dieses Seminar coached Projektleiter in ihrer konkreten Situation der Projektabwicklung ihr eigenes Projekt durch Ausschöpfung des Optimierungspotentials erfolgreicher zu führen.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.290,--

Projekt-Management, 25. - 27.06.01 im Holiday Inn Bonn

In diesem Seminar lernen Projektleiter ein Projekt effektiv zu organisieren und überzeugend zu führen. Es basiert auf einem kreativen Mix aus Lehrvorträgen, Erfahrungsaustausch und praktischen Übungen.
Referent: Dr. Ralf Hillemacher Preis: EUR 1.590,--

Hochverfügbare Netzwerke und Quality of Service, 25. - 27.06.01 im Queens München

Das Seminar beschäftigt sich ausgerichtet auf das Umfeld von "mission critical" Client-Server-Anwendungen mi den Themen High Speed Technik, Ausfall-Sicherheit, Qualitäts-Sicherheit, Garantierbarkeit
Referentin: Dipl.-Inform. Petra Borowka Preis: EUR 1.590,--

Lokale Netze für Einsteiger, 25. - 29.06.01 in der AGIT Aachen

Das Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referent: Dr. Jürgen Suppan Preis: EUR 1.990,--

Aufbau von sicheren IT-Netzen, 27. - 29.06.01 im Queens Hamburg

Das 3-tägige Seminar beschäftigt sich mit den erheblichen Möglichkeiten zur Erhöhung der Sicherheit innerhalb der Lokalen Netzwerke. die moderne Netzwerk-Komponenten und LAN-Technologien bis hin zu den Protokollen bieten.
Referenten: Spezialisten der ComConsult Beratung undPlanung GmbH Preis: EUR 1.590,--

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars _____ Name _____ Vorname _____

Termin _____ Firma, Abteilung _____ Position, Funktion _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____ PLZ, Ort _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/ Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung.

Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht.

Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her.

Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Adapter

Madge, TR-Karten ver. Typen (BM2, MK3, MK4, HSTR) alle PCI, 200 Stck., 60% d. Neupreises B10322

Concentrator

Token Ring Rac 4001 Lan Optics 12 Slot, 5 Stck., DM 400,-- B10305

Hub

Lanstack TR 20 UE,1 Stck., DM 500,-- B10203

Lanstack TR2L, 1 Stck., DM 800,-- B10204

Madge Smart LAM STP, 2 Stck., DM 600,-- B10205

Madge Smart CAu Plus 2 (STP), 1 Stck., DM 500,-- B10206

LET36, 4 Stck., VS B10309

LE20N,16 Stck.,VS B10313

LE 180 XT, 4 Stck., VS B10314

LE140 XTN, 10 Stck., VS B10315

LE140 XT, 12 Stck., VS B10316

Hub

NMAII, 1 Stck., VS B10317

LE10 C2, 2 Stck., VS B10318

LE15, 1 Stck., VS B10319

3Com, Superstack II Hub, LinkBuilder FMS TR, 24- port 4/16 Mbit/s Token Ring Hub, unmanaged, 1 Stck., DM 85,- zzgl. MwSt. B10503

Repeater

AI 3008SL 10, Base 2 Ethernet 8 Port Allied, 1 Stck., DM 350,-- B10323

Ringleitungsverteiler

Madge Smart LAM UTP, 1 Stck., DM 350,-- B10202

Router

RSP2- Board für Cisco 75xx, 8MB onboard Flash, 64MB Memory, 20 MB PCMIA Flash, 1 Stck., VS B10324

Token Ring Einschübe für Rac 4001 12 port Lobemodul 4283 Lan Optics, 20 Stck., DM 400,- bis 700,- B10304

TR LWL Karten BKM 4521 850 Nm 1300 Nm Lan Optics, 10 Stck., DM 400,- bis 700,- B10308

Sternkoppler

Hirschmann ASGE mit diversen Interfacekarten wie: UYDE, CYDE, OYDE, BfOC, KTDE, TYDE, 35 Stck., DM 200,- bis 800,- B10320

Steuereinheit

IBM Token Ring / SNA IBM 3174, 25 Stck., DM 280,- B10303

Switch/Brücke

Cisco Catalyst 5000 Chassis mit 1x WS-X5009 (mit 2x 100 Base TX), 1x WS-5111 (12x 100 Base FX), 1x WS-5213 (12x 100 Base TX), 20MB Memory, V4.5 (7), 1 Stck., EUR 5000,-- B10302

Cabletron 8 Port Ethernet Module for ATX 3E02-08-ATX, 1 Stck., $ 300,- B10310

Switch/Brücke

Cabletron Enhanced ATX Packet Processing Engine 3X00-ATX, 1 Stck., $ 500,-- B10311

Cabletron 3C05-ATX Chassis, inkl. 1 Power Supply 3CPSM-R-ATX, 1 Stck., $ 300,-- B10312

3Com SuperStack Switch 3000, SuperStack 3000, 8- port, 100 Base- TX, vollduplex, VLAN, SNMP, Spanning Tree, 1 Stck., DM 650,- B10502

Handelsplattform für gebrauchte Netzwerkkomponenten

Gesuche

Adapter

IBM Eth. USM Adapter für FDX BNC PT 8274-7100, 1 Stck., VS S10405

IBM, Olicom Token Ring Adapter PCI, 30 Stck., VS S10301

HP J2585B 100VG,160 Stck., DM 80,00 – Kaufen eventuell auch noch 100VG-Hubs wie J2415A sowie Switch 2000 J3100B S10504

IBM, Olicom, Madge TR-Adapter, 16/4, PCI, mit Anschluß SUB D-9, 100 S10402

Concentrator

IBM 8.230.013, 10 bis 50 Stck., DM 400,- S10321

IBM 8.230.013, 10 bis 50, VS S10401

Hub

IBM 8260-3010 Dual Fiber Repeater Module,1 bis 2 Stck.,VS S10404

IBM 8260-3018 18Port TR Media Mod.,1 bis 2 Stck., VS S10403

IBM 8260-1200 DMM Distributed Management Modul, 1 bis 2 Stck., VS S10402

Olicom OC-3626, neu oder gebraucht, 2 Stck., VS S10505

Prozessor

Intel 450 oder 500 MHZ II,1 Stck., DM 200,- S10306

Ringleitungsverteiler

Madge SMART LAM Plus UTP (RJ-45) Nr. 55-50, 1 bis 3 Stck., DM 700,-- S10402

Madge Smart LAN Plus Nr. 55-29, 1 bis 3 Stck., DM 1.200,-- S10201

Madge Smart Lam Plus UTP 55-50, 3 bis 6 Stck., DM 800,- S10307

Router

Cisco Router 2504, IP Feature 2500, ISDN/BRI, 5 Stck., 2000,-- DM S10501

Switch/Brücke

IBM 16 PT RJ 45 UTP/STP 4/16 MBIT TR Switching Modul 8274-0867, 1 Stck., VS S10408

IBM 8 PT 10 Base FL, MMF SC, 2k CAM Switching Modul 8274-0562, 1 Stck., VS S10406

IBM 32-PT 10/100 TX Switching Modul RJ 45 2k CAM 8274-3725, 1 Stck., VS S10407

Fax an 02408/955-399

☐ **Ich suche**
☐ **Ich biete**

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

☐ **Antwort auf Gesuch**
☐ **Antwort auf Gebot**

☐ ☐☐☐☐☐

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon, Fax

eMail

Weitere Gebote und Gesuche

finden Sie auf dem Web-Server der ComConsult Akademie unter

www.comconsult-akademie.de