Dr. Suppan International Institute

Der Netzwerk Insider

Februar 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

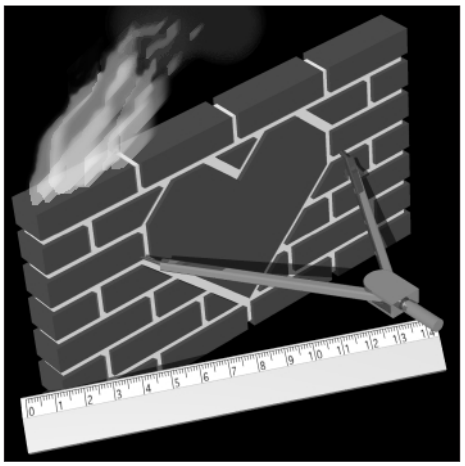
Schwerpunktthema

Firewall-Konfiguration nach Maß: Erfahrungswerte aus der Praxis

von Andreas Meder

Firewalls sind heutzutage aus dem Maßnahmenkatalog zur Sicherung von Netzwerken – zumindest solchen, die nicht nach dem Irischen "Sinn Fein[1]"-Prinzip aufgebaut sind, d.h. als Insel ohne Kontakt zu anderen Netzen – nicht mehr wegzudenken. Entsprechende Systeme sind am Markt in unterschiedlichsten Ausprägungen verfügbar; aus einem Portfolio beginnend bei den eingebauten NAT[2]-Firewalls in DSL-Routern und endend bei mehrstufigen High-End-Systemen gemäß BSI-Empfehlung kann jeder Netzwerkverantwortliche je nach Gusto (und Budget) die geeignete Lösung auswählen. Die Hersteller werben dabei mit Schlagworten wie "Plug & Secure", "Easy Setup" oder dergleichen und suggerieren, Planung und Einsatz einer Firewall wären das reinste Kinderspiel.

Doch leider stimmt das nur bedingt: zwar ist es durchaus richtig, dass die Bedienbarkeit moderner Systeme gegenüber den Anfängen erheblich besser geworden ist, aber unabhängig davon ist es zwecks Optimierung von Sicherheit, Effizienz und Performance unabdingbar, bei der Einrichtung einer Firewall gewisse Grundregeln zu beachten, damit das volle Schutz- und Leistungspotenzial auch ausgenutzt wird.



Das Herzstück der Firewall: auf die inneren Werte kommt es an

Merke: bei einer Firewall zählen primär nicht Äußerlichkeiten, sondern "innere Werte". Dies bedeutet nichts anderes, als dass das gewählte Produkt und die Installationsbasis – Parameter, die sicherlich nicht unwesentlich sind und häufig leidenschaftlich diskutiert werden – in vielen Fällen deutlich weniger Einfluss auf die Leistung des Gesamtsystems "Firewall" haben, als das eigentliche Herzstück: der Regelsatz bzw. die Firewall-Policy, nach der das System die Datenströme behandelt.

Dieser Artikel will zum Verständnis der Problematik beitragen und Anregungen geben, wie man einen effizienten und sicheren Regelsatz aufbaut und pflegt.

weiter Seite 8

[1] Irisch-Gälisch für "Wir selbst allein"
[2] Network Address Translation

Zum Geleit

Schwerpunkt 2003: Ethernet in der Industrie

Ethernet wird seit Mitte der 80er Jahre in der Industrie eingesetzt. Damals führte Siemens als führender deutscher Hersteller in diesem Bereich Ethernet zur Verblüffung der Konkurrenz als Schnittstelle zwischen Leitrechner und großen Steuerungen ein. Doch bis heute wird der eigentliche produktionsnahe Bereich nicht mit Ethernet sondern mit herstellerspezifischen Feldbus-Systemen abgedeckt.

Nun schickt sich Ethernet an, diese letzte Bastion nicht genormter Netze zu sprengen. Mit vielen Vorteilen für Kunden, aber auch für die Hersteller. Keine individuelle, hersteller-abhängige Planung mehr, keine teuren Sonderprodukte mehr.

Statt dessen Einsatz von Standard-Wissen und Standard-Komponenten mit allen bekannten Zusatztools (Analysatoren, Management, Konfiguration, ...) und Betriebshilfsmitteln.

Im Resultat werden Fertigungsnetze besser, beherrschbarer und preiswerter, sowohl in Investition als auch im Betrieb.

Dieser Markt ist so groß und so wichtig, dass auch die großen Netzwerk-Hersteller ihn nicht ohne Kampf an Hirschmann, Siemens, Schneider, Jetter, Rockwell usw. abgeben werden. So werden spätestens in Hannover reihenweise die Ankündigungen für Spezialprodukte im Fertigungsbereich kommen.

Warum Spezialprodukte?

Genau das ist das Problem. Fertigung ist nicht Bürobereich. Standardkonzepte sind schon deshalb nicht einfach übertragbar, weil Fertigungsumgebungen häufig individuell sind. Speziell im Feldbusbereich stehen wir mitten im Anlagenbau. Hinzu kommt, dass auch die bekannten Office-Architekturen häufig nicht übernommen werden können. Auch die Fertigungsnetzwerke selbst bedürfen des Redesigns, sind sie doch entsprechend der bisherigen Hierarchie von Feldbussen und Sensorebene strukturiert. Dabei ergeben sich durchaus Fragen, die auch zu neuen Netzwerk-Konzepten führen müssen.

weiter Seite 2

Schwerpunkt 2003: Ethernet in der Industrie

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

Fortsetzung von Seite 1

Pauschal kann man also sagen, dass die Fertigungs-Netzwerke einem kompletten und komplexen Redesign unterliegen werden, die erprobten Lösungen der Office-Umgebung dafür nicht unbedingt geeignet sind.

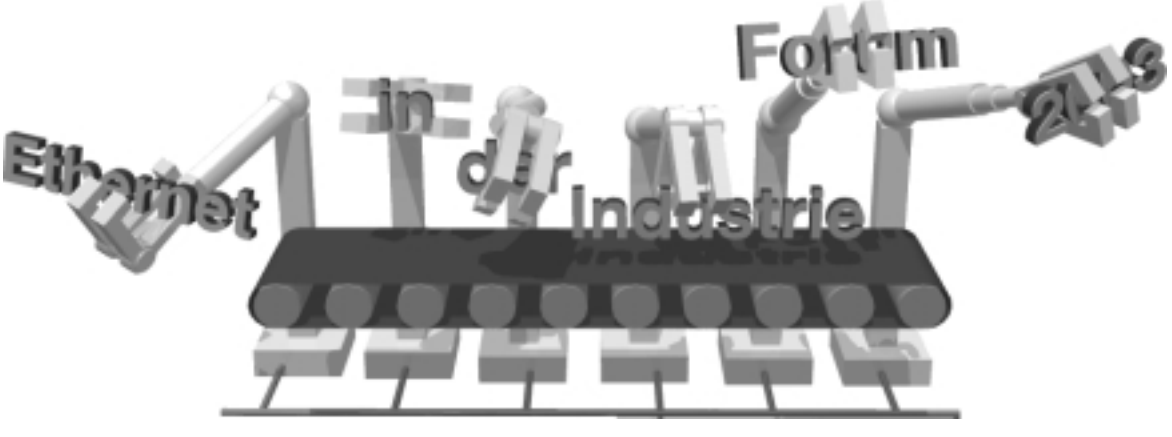
Was ist anders?

- Alle Produkte müssen den verschärften Umgebungsbedingungen im Bereich Schock, Vibration, Temperatur, Feuchtigkeit entsprechen. Im Zweifelsfall müssen die gängigen IEC-Normen für Steuerungen eingehalten werden.
- Produkte müssen andere Architektur-Eigenschaften hinsichtlich Schnittstellen, Netzteil, Verfügbarkeit erfüllen.
- Die traditionellen Switching-Verfahren à la Spanning Tree, OSPF usw. haben im Feldbus-Bereich nichts verloren. Was aber dann?
- Verkabelungs-Lösungen sind anders, RJ45 in seiner Reinform für harte Bedingungen ungeeignet.
- Architekturen sind anders. Hier dominieren Busstrukturen und keine Sterne.
- Stromversorgung ist anders. 24 V Externversorgung ist eine denkbare Forderung.
- Montage ist anders. Die Hutschiene lässt grüßen.
- Es bestehen Realzeitanforderungen, die im Extremfall bis in den Mikrosekunden-Bereich gehen (Motion Control).
- TCP/IP ist sicher nicht immer in der Lage, diese Anforderungen zu erfüllen. An einem Ersatz arbeiten mehrere Hersteller.
- Eine Migration vom Feldbus zum Ethernet ist erforderlich.
- Die Tools der Anlagenplanung, auf deren Basis die komplexen Anlagen- und Automatisierungsabläufe geplant und realisiert werden, müssen erneuert werden. Dabei werden sie automatisch komplexer, da durch die Aufhebung der Feldbus-Inseln jetzt der Bedarf nach einer Komplett-Projektierung entsteht. Damit werden auch die Projektierungstools wesentlich umfangreicher und leistungsstärker werden müssen. – Aber genau hier liegt einer der zentralen Vorteile für den Anwender.

Somit liegen eine Reihe von Aufgaben vor uns, die wir bearbeiten müssen. Wir haben ein Spezialisten-Team gebildet, das sich in den nächsten Monaten um dieses Thema kümmert. Die Ergebnisse präsentieren wir Ihnen auf unserer Sonderveranstaltung "Ethernet in der Industrie Forum 2003" vom 5. bis 7. Mai in Königswinter.

Ihr
Dr. Jürgen Suppan

(drsuppan@comconsult-akademie.de)



Anzeige

10 % Frühbucherrabatt bis 15.03.03

Ethernet in der Industrie Forum 2003

05.05. - 07.05.03 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir exklusiv eine Vorbuchungsphase für die Sonderveranstaltung "Ethernet in der Industrie Forum 2003" bis zum 15.03.2003 für eine rabattierte Teilnahmegebühr an. Versäumen Sie daher nicht, sich rechtzeitig einen Platz auf dieser Veranstaltung zu sichern und nutzen Sie dazu jetzt noch den Sonder-Rabatt. Lassen Sie sich diesen herausragenden Kongress nicht entgehen!

3 Tage Ethernet in der Industrie Forum 2003
zum Preis bei Buchung bis 15.03.03 von € 1.430,-- statt regulär € 1.590,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sonderveranstaltung Ethernet in der Industrie Forum 2003

☐ Ja, ich möchte den Vorbuchungs-Rabatt nutzen und buche verbindlich die **Sonderveranstaltung Ethernet in der Industrie Forum 2003** vom 05.05. - 07.05.03 in Königswinter zum Preis von € 1.430,-- (statt 1.590,--)

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel Königswinter (€ 110,-- pro Übernachtung mit Frühstück)

von _____ bis _____

*Frühbucherpreise nur gültig bis 15.03.03

Buchen Sie über unsere Website: **www.comconsult-akademie.de**

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

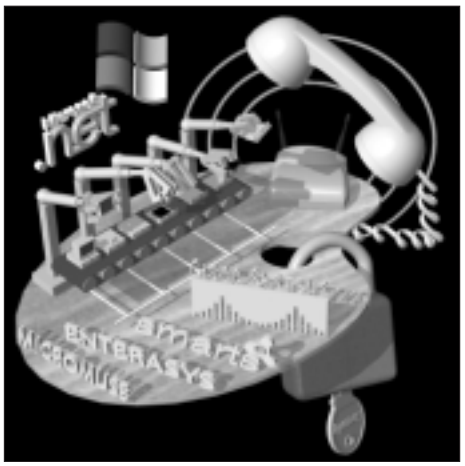
Aktueller Kongress

Netzwerk-Redesign Forum 2003

Die Vorbereitungsarbeiten auf das Top-Forum des Jahres, das Netzwerk-Redesign Forum 2003 vom 7. bis 10. April laufen auf Hochtouren. Wie in jedem Jahr, so werden wir auch diesmal wichtige Analyse-Ergebnisse, Labor-Untersuchungen sowie Produkt- und Technologie-Bewertungen auf diesem Forum veröffentlichen.

Bei den laufenden Arbeiten zeichnen sich neben den schon veröffentlichten Schwerpunkten folgende Highlights ab:

- Bei der Ethernet-Standardisierung haben sich massive und wichtige Neuerungen ergeben. Auch im Bereich IEEE 802.1D wird es gravierende Änderungen geben.
- Unser Labor hat eine neue Messreihe zu Kabelkomponenten aufgelegt, um die Konformität der Produkte mit der neuen EN 50173 zu testen.
- Messtechnik und Analyse im WLAN-Umfeld hat sich als besondere Herausforderung erwiesen, unsere Spezialisten berichten über Erfahrungen und geben Empfehlungen für die optimale Messtechnik.
- Die Wirtschaftlichkeit des Netzwerk-Betriebs lässt sich durch optimiertes Design und die konsequente Nutzung neuester Management-Ansätze deutlich verbessern. Ein Anwender berichtet, wie ein überregionaler landesweiter Flächenbetrieb massiv optimiert und mit minimaler Personenzahl umgesetzt werden konnte.



- Eine laufende Untersuchung zu Sicherheits-Lücken in unseren Client/Server-Architekturen hat eine klar dominierende Schwachstelle für fast alle größeren Umgebungen ergeben. Lösungsansätze werden mit Ihnen diskutiert.
- Ethernet verdrängt den Feldbus in industriellen Umgebungen. Das Thema ist kritisch, zeigen doch Untersuchungen, dass das damit verbundene TCP/IP einer Reihe von Realzeitaufgaben nicht gewachsen ist. Wir diskutieren diese Situation und zeigen die zur Zeit in Arbeit befindlichen Lösungsansätze auf.

.

- Zur Zeit wird eine tiefgehende Studie zum Thema: "Kann Wireless die bestehenden kabelgebundenen Netzwerke verdrängen" durchgeführt. Schon jetzt ist sichtbar, dass die Ergebnisse für erheblichen Aufruhr sorgen werden, sehen Sie an dieser Stelle mit großer Spannung dem Forum entgegen.
- Die Integration von Rechenzentren erfordert ein weitergehendes Netzwerk-Design. Wir stellen die gegebenen Möglichkeiten vor und geben Empfehlungen
- Corporate Networks sind technisch im Umbruch, die Virtualisierung von Unternehmen zwingt zu neuen Strukturen. Auf der Basis aktueller Großprojekte zeigen wir die bestehenden Möglichkeiten auf

Das ist nur ein Auszug aus den zur Zeit für Sie laufenden Arbeiten. Wir gehen davon aus, dass dies eines der spannendsten und interessantesten Foren der letzten Jahre wird.

Nach der jetzigen Buchungslage wird die Veranstaltung ausgebucht sein. Zögern Sie also nicht, sich rechtzeitig einen Platz auf unserer Top-Veranstaltung des Jahres 2003 zu sichern.

Netzwerk-Redesign Forum 2003 – Die Inhalte

Montag, den 07.04.03: Technologie-Entwicklung und Standardisierung

Technologie-Trends 2003:
- Die aktuellen Trends bei Server und Clienten
- Neue Software-Architekturen: warum wichtig?
- Speicher-Technologien im Netzwerk
- Desaster-Recovery
- Unternehmens-Virtualisierung
- Konsequenzen für Netzwerk-Technologien
- Technologie-Trends Netzwerke

Dr. Jürgen Suppan
{ComConsult Technologie Information)

Aktuelle Aktivitäten bei IEEE 802:
Woran wird z. Zt. gearbeitet und was steckt dahinter?
- Wie ist der aktuelle Stand der Normierung und wann kommt es?
- Was ist wichtig?
- Wer steckt dahinter?

Thomas Schramm
(Hirschmann)

Neue Ethernet-Technologien
- Perspektiven der Ethernet-Entwicklung
- Technologische Hintergründe
- 10 Gbit/s über Kupfer: Wie funktioniert es, wo nutzbar, neue Perspektiven für Server und Speicher?
- 100 Gbit/s
- First Mile

Dr. Franz-Joachim Kauffels

Die richtige Entscheidung treffen bei der Auswahl von Kategorie-6-Systemen und Glasfasern
- Welche Kategorie-6-Auswahlkriterien gibt es
- Was bringt ein "Kategorie-6-De-Embedded-System"
- Laborerfahrungen mit so genannten "De-Embedded-Systemen"
- Gibt es Weiterentwicklungen bei Kategorie-6-Systemen?
- Vergleich der OM1, OM2, und OM3-Fasern bei Nutzung von Ethernet
- Welche Singlemodefaser ist im LAN die richtige?

Dipl.-Ing. Hartmut Kell
(ComConsult Beratung und Planung)

Netzwerk-Redesign Forum 2003

Dienstag, den 08.04.03: Optimierung des Betriebs und Nutzung neuer Potenziale

Potenziale des Netzwerk-Designs optimal ausschöpfen
- Was Netzwerk-Design leisten kann
- Migration von "Altlasten" (Token Ring, ATM)
- Design-Alternativen neuester Stand: L2, L3, VLANs, Redundanzverfahren
- Optimierungs-Kriterien: Wirtschaftlichkeit, Performance, Verfügbarkeit, Realzeit/ Multimedia, Einfacher Betrieb
- Typische Beispiele
- Was kommt auf uns zu/neue Standards • Trendausblick

Dipl.-Inform. Petra Borowka (UBN)

Schlüsseltechnologie: Netzwerk-Management
- Warum Schlüsseltechnologie?
- SNMP-Management als Schwachstelle des modernen Managements
- Warum eine SNMP-Konsole nicht ausreicht
- Gegenüberstellung der Alternativen
- Rolle der herstellerspezifischen Tools
- Wo steht die LAN-Analyse
- Gesamtkonzept

Dr. Jürgen Suppan (ComConsult Technologie Information)

Wirtschaftliche Optimierung des Netzwerk-Betriebs
- Ausgangslage
- Zielsetzung: landesweiter Flächenbetrieb mit wenig Personal
- Warum die traditionellen Ansätze nicht ausreichen
- Lösungs-Ansatz
- Netzwerk-Betrieb im Rechenzentrum der Finanzverwaltung
- Bewertung

Karl-Heinz Hommen-Menz (RFZ NRW)

Analyse und Messtechnik für WLAN-Netzwerke
- Warum WLAN-Netzwerke kritischer sind als kabelgebundene
- Typische Szenarien bei der WLAN-Analyse
- Zwischen Sniffer und Spectrum-Analyzer: Welches Tool für welche Aufgabe?
- "Wer misst, misst Mist": Praktische Tipps für WLAN-Messungen
- Was kostet die Analysetechnik?
- Messen in der Grauzone: Was sagt der Gesetzgeber?
- Fazit und Empfehlungen

Dr. Joachim Wetzlar (ComConsult Beratung und Planung)

Sicherheit in vernetzten Microsoft Umgebungen: wo liegt die Hauptschwachstelle?
- Welche Technologien beeinflussen Sicherheit?
- Wie ist die Situation in den Technologien zu bewerten?
- Wo ist unsere Hauptschwachstelle und warum ist das so?
- Ansatzpunkte zur Beseitigung der Schwachstelle
- Projekterfahrungen und Empfehlungen

Michael van Laak (ComConsult Beratung und Planung)

Connectivity, Mobility, Security: Auf dem Weg zum virtuellen Unternehmen
- Was bedeuten Connectivity und Mobility?
- Welche Möglichkeiten zur standortübergreifenden Kommunikation gibt es?
- Typische Szenarien
- Schlüsselfaktoren Flexibilität, Sicherheit, Kosten
- Lösungsansätze
- Projekterfahrungen

Dr. Behrooz Moayeri (ComConsult Beratung und Planung)

Mittwoch, den 09.04.03. Neue Technologien in der Praxis

Voice over IP gezielt und erfolgreich einsetzen
- VoIP-Lösungen setzen sich durch
- Aktuelle Entwicklungen und Trends
- Alternative Lösungsansätze
- Wer sollte wann was tun?
- Empfehlungen

Dipl.-Inform. Petra Borowka(UBN)

Wireless-Netzwerke zielgerichtet und betriebssicher umsetzen
- Wireless Technologie-Varianten
- Wer wird sich durchsetzen?
- Bekannte Probleme bei neuen Technologien
- Planungs-Methoden
- Betriebs-Problematik
- Ausblick

Dr. Simon Hoff(ComConsult Beratung und Planung)

Ethernet in der Industrie
- Ethernet dringt in den Feldbus vor
- Was unterscheidet Office und Industrial Ethernet?
- Welche Verkabelung, was müssen Komponenten können?
- Welchen Einfluss haben Echtzeit-Anforderungen
- Wo steht Siemens als Marktführer?
- Trends und Strategien?

Manfred Fürsattel, Christof Kreienmeier (Siemens)

RZ-Integration in Netzwerke optimal umsetzen
- Welche besonderen Anforderungen stellen RZ-Umgebungen an Netzwerke
- Wie werden Server optimal in Netzwerke integriert
- Wo liegen Unterschiede zwischen den Betriebssystemen
- Welche Bedeutung hat IP-Management
- Wo sollte der Internet-Zugang gestaltet werden, welchen Stellenwert haben Carrier-Redundanz und Hardware-Redundanz
- Schlüsseltechnologie Desaster-Recovery
- Lösungsansätze und Erfahrungen

Dr. Behrooz Moayeri (ComConsult Beratung und Planung)

Corporate Networks im Umbruch
- Ausgangslage
- Verfügbare Technologien
- Warum die traditionellen Ansätze ggf. nicht mehr geeignet sind
- Alternativen
- Kriterien und ihre Konseqenzen
  - Kosten
  - Internationale Strukturen
  - Performance
  - Internet-Nutzung/Zugang
- Fazit und Empfehlungen

Dr. Behrooz Moayeri (ComConsult Beratung und Planung)

Netzwerk-Redesign Forum 2003

Donnerstag, den 10.04.03: Workshops und Vertiefung

Workshop 1: Wireless LANs
(Dr. Simon Hoff, Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan)

- Wie Wireless-Technologien arbeiten
- Wo die gravierenden Schwachstellen der eingesetzten Verfahren liegen und warum Sie dieses kennen müssen
- Wie der Markt aussieht und wie er sich entwickelt
- Wie die neuen Varianten arbeiten und welche Vorteile sie haben
- Warum Sie sich bewusst für ein Codierungs-Verfahren entscheiden müssen und warum dies hier keine reine theoretische Frage ist
- Wann und warum welche Produkte mit welcher Technologie zwischen den Herstellern interoperabel sind und wo dies zur Zeit nichtgesichert ist
- Wie Sie erfolgreiche eine flächendeckende Versorgung planen und realisieren können
- Warum eine Planung auf der Basis einer Antennen-Abdeckung unzureichend sein kann
- Warum die Planung der Antennen-Montage-Punkte je nach eingesetzter Technologie äußerst kritisch sein kann
- Wie die häufig diskutierten Sicherheits-Bedenken zu bewerten sind und wie Sie Ihre Installation sicher machen können
- Was bei einer Installation in speziellen Umgebungen wie medizinische Bereiche oder Personalverwaltung oder Schule mit erheblichen Auflagen des Bundesdatenschutzgesetzes zu beachten ist und ob und wenn ja, wie dort eine Wireless-Installation sinnvoll erfolgen sollte
- Welchen hohen Stellenwert das Distribution-Netzwerk für eine flächendeckende Installation hat und wie Sie dabei die sehr häufig gemachten Auslegungsfehler vermeiden können
- Wie sich typische Produkte des Marktes im Labortest verhalten und was das für die tägliche Praxis bedeutet

Workshop 2: Voice-over-IP
(Dipl.-Inform. Petra Borowka)

Zur Marktsituation:
- Wo steht VoIP, was bedeuten die neuen Entwicklungen?
- Wird es in kurzer Zeit VoIP-Lösungen von der Stange geben?
- Wie entwickelt sich der Endgerätemarkt, und wann: Softphones, PDAs, Screenphones?
- Welche Konsequenzen hat der Einsatz von VoIP für das Netzwerkmanagement?

Zur Standardisierung:
- Was leistet die aktuelle Standardisierung?
- Was bedeutet der Umstieg auf SIP? Ist das Ende der Hersteller-spezifischen Lösung nahe?
- Ist mit einer deutlichen Vergrößerung des Leistungsumfanges standardisierter Lösungen zu rechnen? Wenn ja, wann?
- Was ist von Wireless VoIP zu halten?

Zu den Key Playern:
- Was bringt der Einstieg von Microsoft und Intel dem Markt?
- Was bedeutet die SALT Initiative?
- Was bieten die großen Hersteller? Wie sind die aktuellen Produktlinien zu bewerten? Wer hat die Nase vorn?

Zur Projektdurchführung:
- Welche Vorteile entstehen wann und für wen?
- Welche Erfahrungen wurden in den bisherigen Projekten gemacht?
- Was ist beim Betrieb einer VoIP-Lösung zu beachten?

Zur Kostensituation: Wie entwickeln sich Preise und Leistungen?
- Sind weitere dramatische Preissteigerungen zu erwarten?
- Wo steht der Kostenvergleich zwischen klassischem PBX-Einsatz und VoIP-Lösung?

Fax-Anmeldung an ComConsult 02408/955-399

Netzwerk Redesign-Forum 2003
07.04. - 10.04.03 in Königswinter

Ich melde mich an für das
Netzwerk-Redesign Forum 2003

☐ **vom 07.04. - 10.04.03 mit Workshop**
☐ **Wireless LANs**
☐ **Voice-over-IP neuester Stand**
zum Preis von € 1.790,-- zzgl. MwSt.

☐ **vom 07.04. - 09.04.03 ohne Workshop**
zum Preis von € 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel Königswinter
(€ 110,-- pro Übernachtung mit Frühstück)

von _____ bis _____

Buchen Sie über unsere Website:
www.comconsult-akademie.de

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

Neuer Technologie Report

Voice-over-IP: Anforderungs-Katalog und Evaluierung

Der brandneue Report der ComConsult Technologie Information "Voice-over-IP: Evaluierung" setzt sich kritisch mit dem Thema Voice-over-IP auseinander. Er zeigt, wann ein Einsatz sinnvoll ist und wann sie mit ihrer Entscheidung noch warten sollten.

Eigentlich ist Markt reif für VoIP:

- Fast alle TK-Hersteller haben ihre Produkte mit VoIP-Fähigkeiten versehen.
- Viele der zukünftigen Multimedia-Anwendungen werden auf VoIP-Diensten basieren.
- Mehr und mehr Anwender integrieren VoIP in ihr Lösungs-Portfolio.
- Die Produkte schwenken auf SIP um, eine wesentliche Voraussetzung für eine genormte TK-Funktionalität.
- Die Kosten für VoIP-Lösungen sinken.

Trotzdem ist eine Entscheidung für Voice-over-IP nicht leicht. Immer noch gibt es eine Reihe ernstzunehmender Kriterien, die auch gegen einen Voice-over-IP-Einsatz sprechen können.

Hier setzt der Report "Voice-over-IP: Evaluierung" an. Dieser Report zeigt Ihnen:

- was hinter Voice-over-IP steckt
- nach welchen Kriterien eine Entscheidung für eine neue TK-Lösung fallen sollte

Aktueller Report

- wie Sie bei der Auswahl einer neuen TK-Lösung vorgehen können
- wie eine VoIP-Lösung nach diesen Kriterien zu bewerten ist
- wo die Schwachstellen einer VoIP-Lösung liegen
- was hinter dem Normungsstreit SIP kontra H.323 steckt
- wie der Markt einzuschätzen ist
- wie die Kosten einer traditionellen TK-Lösung gegenüber VoIP zu bewerten sind
- wo wichtige Hersteller wie Avaya, Alcatel, CISCO, Nortel und Siemens stehen

Dabei wird auch auf folgende Fragen eingegangen:

- Mit welchen Vor- und Nachteilen sind IP-PBX-Lösungen zum jetzigen Zeitpunkt hinsichtlich Leistungsmerkmale, Sicherheit, Verfügbarkeit, Skalierbarkeit etc. verbunden?
- Welche Vorteile bieten IP-PBX-Systeme für Unified Messaging und Call-Center-Anwendungen?
- Stellt das Ersetzen des Zweidrahttelefons mit einem kleinen Display und einer numerischen Tastatur durch ein IP-Telefon mit einem etwas größeren Display und einer numerischen Tastatur für den Anwender eine ausreichende Motivation dar, zu VoIP zu migrieren?
- Was muss die Zielsetzung der VoIP-Migration sein?
- Wie weit sind wir von einer offenen, standardisierten Welt im Bereich VoIP entfernt?
- Was ist der Migrationspfad zum Erreichen der offenen, standardisierten Umgebung?
- Ausblick auf Signalisierungsstandards und Verbesserung der Leistungsmerkmale der IP-PBX-Lösungen, z. B. durch Verfügbarkeit neuer Applikationen, deren Einsatz im Unternehmen sinnvoll und vorgesehen sind

Für jeden, der in der Entscheidung für eine neue TK-Lösung steht, ist dieser Report ein unverzichtbares Hilfsmittel.

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung

Ich bestelle den Technologie Report

☐ **Voice-over-IP Evaluierung**
zum Preis von € 349,--
zzgl. MwSt. und Versandkosten

_____
Unterschrift

_____
Name, Vorname

_____
Firma, Abteilung

_____
Straße

_____
PLZ, Ort

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von € 5,-- zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports € 10,-- zzgl. MwSt. (Bei Versendungen ins Ausland € 25,-- bzw. bei 2 oder mehr Reports € 30,-- zzgl. MwSt.)

Firewall-Konfiguration nach Maß: Erfahrungswerte aus der Praxis

Fortsetzung von Seite 1

Immer schön der Reihe nach...

Der Regelsatz (die "Rulebase") der Firewall bestimmt, wie sie mit den Datenpaketen bzw. Kommunikationsverbindungen, die sie auf Zulässigkeit prüft, umzugehen hat: dazu wird festgelegt, welche Eigenschaften ein Datenpaket aufweisen muss, damit es eine bestimme Behandlung erfährt - z.B. könnte eine solche Festlegung lauten: Datenpakete, die zum E-Mail-Versand aus dem eigenen Netz ins Internet dienen, dürfen die Firewall passieren, werden aber protokolliert.

Nahezu alle Firewalls arbeiten dabei nach einem einheitlichen Prinzip mit zwei Grundregeln:

- Sie arbeiten ihren Regelsatz sequentiell ab.
- Der Vorgang endet, sobald eine passende Regel gefunden wurde.

Hieraus lassen sich unmittelbar einige wichtige Designregeln für einen effizienten Regelsatz ableiten:

- Je genauer eine Regel die passenden Datenpakete eingrenzt, desto weiter oben (d.h. vorne) im Regelsatz muss sie auftauchen, da sie ansonsten von ähnlichen, aber nicht so eng gefassten Regeln "ausgeblendet" wird. Dazu ein Beispiel: Will man den Web-Zugriff prinzipiell erlauben, für einen bestimmten Rechner aber ausschließen, so muss die ausschließende Regel (A), weil sie die in Frage kommenden Datenpakete enger eingrenzt, vor der erlaubenden Regel (B) im Regelsatz auftauchen; andernfalls wird ein Datenpaket nach Regel B durchgelassen, selbst wenn es nach Regel A verboten wäre – Regel A kommt einfach gar nicht mehr zum Zuge...
- Je häufiger eine Regel voraussichtlich zutrifft, desto weiter oben im Regelsatz sollte sie auftauchen; dadurch reduziert man die Bearbeitungsschritte, die die Firewall leisten muss. Auch hierzu ein Beispiel: Besteht der Datenverkehr hauptsächlich aus Web-Zugriffen, so sollten die Regeln A und B aus obigem Beispiel weit vorne in der Rulebase stehen; andernfalls muss bei den meisten Datenpaketen stets ein großer Teil der Rulebase unnütz abgearbeitet werden, bis die passenden Regeln gefunden sind.
- Die Gesamtlänge des Regelsatzes, d.h. die Anzahl der darin enthaltenen Regeln hat maßgeblichen Einfluss auf die Performance der Firewall. Es wird stets Datenverkehr geben, der nicht speziell durch eine darauf zugeschnittene weit vorne platzierte Regel erfasst werden kann – hierzu zählen insbesondere unangeforderte Datenpakete aus dem Internet, die typischerweise durch eine abschließende Regel, die alles verbietet, behandelt werden. Für solchen Datenverkehr muss stets der gesamte Regelsatz abgearbeitet werden.

In der Kürze liegt die Würze...

Neben dem zuvor genannten Aspekt spricht noch ein weiterer wichtiger Grund für die Verwendung möglichst kurzer Regelsätze: sie sind wesentlich übersichtlicher als lange Regelsätze und deshalb leichter beherrschbar. Dadurch vereinfacht sich der Betrieb der Firewall, die Ursachenforschung im Fall von Kommunikationsproblemen wird beschleunigt, und die Gefahr von Konfigurationsfehlern sinkt. Firewall-Regelsätze sollten daher so kurz und einfach wie möglich gehalten werden. Man sollte dabei auch im Auge behalten, dass Firewalls oft von mehr als einer Person betrieben werden, insbesondere, wenn sie über einen längeren Zeitraum im Einsatz sind. Je einfacher der Regelsatz strukturiert ist, desto leichter findet sich ein neuer Administrator darin zurecht...

Zur Verdeutlichung des Einflusses der Übersichtlichkeit des Regelsatzes auf die Fehlerfreiheit – und damit potentiell auf die Sicherheit des Netzwerks – mag ein kleines Beispiel dienen, das auf einer wahren Begebenheit beruht, die dem Autor bei der Untersuchung der Firewall einer großen deutschen Tageszeitung widerfuhr:

Stellen wir uns eine Firewall mit umfangreichem Regelsatz vor, in dem sich unter anderem eine Regel befindet, die es gestattet, aus dem Internet auf spezielle Ablageserver für den Datenaustausch zuzugreifen; diese Server befinden sich in einem speziellen Netzbereich. Der Einfachheit halber – eigentlich ein lobenswerter Ansatz (siehe oben), aber übertreiben darf man es natürlich auch nicht – hat man auf eine Einschränkung der Art des Zugriffs verzichtet. An anderer Stelle findet sich eine Regel, die die Kommunikation dieser Ablageserver mit internen Servern gestattet; diese Regel ist prinzipiell notwendig, um den Datenfluss zu ermöglichen. Auch hier wird nach obigem Prinzip die Kommunikationsform nicht eingeschränkt.

Beide Regeln für sich betrachtet stellen kein Risiko dar. Zusammengenommen erlauben sie jedoch den Zugriff aus dem Internet auf Server im internen Netzwerk beispielsweise über Telnet – ein Szenario, das in dieser Form sicherlich nicht beabsichtigt war.

Das Problem wäre bei besserer Übersichtlichkeit des Regelsatzes wohl deutlich eher aufgefallen...

Beachten Sie bei der Überlegung, welche Anzahl von Regeln für Sie noch beherrschbar ist, auch noch eine weitere Eigenschaft von Systemkonfigurationen: Sie neigen dazu, monoton zu wachsen, d.h. es kommen im Laufe der Zeit mehr und mehr Regeln hinzu. Dies liegt daran, dass nur selten vorhandene Regeln gelöscht aber häufig neue Regeln hinzugefügt werden. Ein Kunde des Autors stellte beispielsweise im Verlaufe eines Audits seiner Firewall erstaunt fest, dass einige Regeln scheinbar überhaupt keinen Sinn hatten. Des Rätsels Lösung: sie waren über ein Jahr zuvor als Übergangslösung implementiert und niemals wieder entfernt worden...

Der Autor

Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security.

Firewall-Konfiguration nach Maß: Erfahrungswerte aus der Praxis

Natürlich lässt sich die Forderung nach einem kurzen Regelsatz nicht immer umsetzen. Je nach Einsatzszenario kann es unumgänglich sein, eine Vielzahl unterschiedlichster Kommunikationsbeziehungen zu reglementieren, so dass in komplexeren Umgebungen Regelsätze mit 100 oder mehr Regeln durchaus vorkommen. Der Regelfall ist dies jedoch sicherlich nicht. In einfachen Umgebungen mit typischem Einsatzfall kommt man meist mit 10 bis 15 Regeln aus; mehr als 25 bis 30 sind selten wirklich notwendig. Oft resultieren umfangreichere Regelsätze aus viel zu detaillierten Sicherheitsrichtlinien, deren effektiver Gewinn für die Gesamtsicherheit des Netzwerks höchst fragwürdig ist; bei Vereinfachung – etwa durch Wegfall unnützer Ausnahmeregelungen – kann die Regelmenge oft deutlich reduziert und damit sowohl die Firewall als auch ihre Administratoren spürbar entlastet werden.

Der Chef sagt (hoffentlich), wo's lang geht...

Unabhängig davon, wie kurz oder wie lang, wie einfach oder komplex ein Firewall-Regelsatz aufgebaut ist, muss stets eine entsprechende Grundlage für seine Definition vorhanden sein. Anders ausgedrückt: Bevor man eine Firewall mit einem Regelwerk ausstattet, das die Sicherheitsregularien umsetzt, die für das Netzwerk gelten, müssen diese Regularien überhaupt erst einmal vorhanden sein. Das klingt nach einer Selbstverständlichkeit, in der Praxis trifft dies aber oft genug nicht zu: zwar existieren Sicherheitsrichtlinien oder -bestimmungen, aber diese wurden von den Administratoren der Sicherheitssysteme definiert – stets bedarfsorientiert und punktuell, oft sogar auf die aktuelle Konfiguration zugeschnitten: nicht das Sicherheitsbedürfnis des Netzes bestimmt die Schutzmaßnahmen, sondern die vorhandenen Mechanismen definieren Schutzbedarf und Spielregeln nach dem Motto "Dieses und Jenes ist bei uns erlaubt, weil unsere Firewall das nicht unterbinden kann...". Eine solche Vorgehensweise mag hochgradig praktikabel sein, birgt aber Risiken: zum einen entspricht der tatsächliche Schutzlevel oftmals nicht dem eigentlichen Bedarf, zum anderen wird er durch ständiges Nachbessern immer wieder verändert und dabei in aller Regel abgesenkt.

Der einzig gangbare Weg aus dieser Misere besteht darin, dass die Sicherheitsrichtlinien die Grundlage für die Firewall-Konfiguration sein müssen und nicht umgekehrt. Dazu ist es unbedingt notwendig, dass diese Richtlinien seitens der Geschäftsführung verbindlich festgeschrieben werden, um jeglichem Gerangel um deren Angemessenheit und Sinnfülle von vorneherein den Nährboden zu entziehen. Kurz gesagt: Der Chef bestimmt, was zulässig ist und was nicht, und die Firewall-Regeln legen fest, auf welche Weise dies durchgesetzt wird. Leider neigt die Chefetage dazu, sich aus dem notwendigen Prozess zur Definition dieser Richtlinien auszuklinken – aus ihrer Sicht nicht einmal völlig zu unrecht, denn die Erarbeitung einer solchen Sicherheitspolitik, insbesondere, wenn sie einigermaßen umfassend sein soll, ist aufwändig und Chef-Arbeitsstunden sind teuer; auch das Argument, dass man mangels Sachkenntnis ohnehin nichts beitragen könne, wird gerne genutzt - in diesem Fall sollte der für die Umsetzung Verantwortliche zumindest die von ihm selbst als sinnvoll erachteten Regularien vom Management formal absegnen lassen. Dies liefert ihm erstens eine gewisse Absicherung für den Fall, dass die Sicherheitsmechanismen sich einmal als unzureichend erweisen sollten und gibt ihm zweitens ein Mittel an die Hand, sich gegen Versuche, die Regeln aufzuweichen, zur Wehr zu setzen.

Von den Sicherheitsrichtlinien zur Firewall

Wie generiert man nun aus den Bestimmungen der Sicherheitspolitik eine Architektur und ein Regelwerk für die Firewall? Dazu betrachten wir am besten ein kleines Beispiel, an dem sich die wesentlichen "Knackpunkte" einer effizienten Regelbasis herausarbeiten lassen.

Wir stellen uns zunächst die Sicherheitsbestimmungen eines exemplarischen Unternehmens als Ausgangsbasis vor:

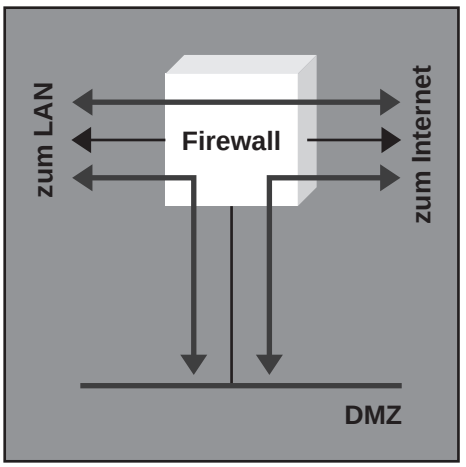
1. Die Nutzung von Web-Diensten (HTTP, FTP) ist für alle internen Anwender erlaubt.
2. Ein Zugriff von außen auf das interne Netz ist nur für authentifizierte Anwender gestattet.
3. Der sichere E-Mail-Verkehr mit dem Internet ist zulässig.
4. Ein Zugriff von außen auf eigene öffentliche Server (Webserver etc.) ist zulässig.

Natürlich können reale Sicherheitsbestimmungen sehr viel umfangreicher und auch komplexer ausfallen – je nach Sicherheits- und Kommunikationsbedürfnis des betrachteten Unternehmens. Für unsere Zwecke reicht dieses Szenario jedoch völlig aus.

Der erste Schritt ist nun die Gestaltung der Firewall-Architektur, die die beschriebenen Sicherheitsbestimmungen umsetzen soll. Als Firewall-Basis gehen wir von einem Dynamischen Paketfilter aus, einem weit verbreiteten Firewall-Typ (wir werden noch sehen, dass wir zur vollständigen Umsetzung der Sicherheitsbestimmungen etwas erweiterte Funktionalität der Firewall benötigen, aber dazu später mehr...). Dynamische Paketfilter besitzen gegenüber normalen, statischen Paketfiltern den unschätzbaren Vorteil, dass sie Antwort-Datenpakete den anfragenden Paketen zuordnen können. Dadurch entfällt die Notwendigkeit, spezielle Firewall-Regeln für diese Antworten zu definieren, wodurch sich der Konfigurationsaufwand verringert, der Regelsatz verkürzt und last but not least die Sicherheit nicht unbeträchtlich erhöht: anstelle einer statischen Regel, die potentielle Antwortpakete aus beliebigen Quellen mit nicht vorher bestimmbaren Kommunikationsports zulassen muss, erzeugt eine solche Firewall dynamisch, d.h. zur Laufzeit, zu jedem Paket, das die Firewall auf Basis einer statischen Regel passieren darf, eine passende Antwortregel, die auf genau eine Kommunikationsbeziehung beschränkt ist.

Diese Firewall statten wir nun mit (mindestens) drei Netzwerk-Interfaces aus. Ein Interface stellt die Anbindung an das Internet her, ein weiteres die Anbindung zum internen Netz. Das dritte Interface dient der Realisierung einer so genannten Demilitarisierten Zone (DMZ) – hierbei handelt es sich um einen Netzwerkbereich, der weder dem internen noch dem externen Netz angehört. Eine Kommunikation mit dieser DMZ muss bei einer solchen Architektur zwingend über die Firewall abgewickelt werden, so dass eine Kontrolle des Datenverkehrs mit der DMZ sichergestellt ist (Bild 1).

Bild 1 Firewall-Topologie und Kommunikationskontrolle



In dieser DMZ werden wir alle unsere Systeme aufstellen, die in exponierter Weise Kontakt mit dem Internet haben sollen. Dazu gehören insbesondere alle öffentlichen Server, also z.B. der eigene Web-Server.

Nachdem wir nun die grobe Topologie unserer Firewall-Architektur festgelegt haben, geht es an die Umsetzung der Sicherheitsbestimmungen.

Bestimmung 1 gestattet die Nutzung des Internet für alle internen Anwender. Zur Erhöhung von Sicherheit und Performance wird dieser Zugriff über einen internen Proxy-Server, der gleichzeitig als Web-Cache fungiert, realisiert. Die notwendige Namensauflösung wird über einen internen und einen externen DNS-Server abgewickelt: Interne Web-Browser stellen ihre Anfragen an den internen DNS-Server, der diese - je nach gesuchtem Ziel – entweder selbst beantwortet (Bild 2) oder aber bei Bedarf über den externen DNS-Server an das Internet weiterleitet (Bild 3).

Grundsätzlich kann man dies auch einfacher gestalten, etwa über direkte Anfragen der Browser an DNS-Server im Internet; da die DNS-Server-Struktur aber ohnehin vorhanden ist - ohne internen DNS-Server kommt man kaum mehr aus und der externe wird durch Sicherheitsbestimmung 4 in Verbindung mit Bestimmung 2 motiviert – sollte man sie auch nutzen, um die Sicherheit zu erhöhen.

Eine solche Kaskadierung (vgl. Bild 4) verringert das Angriffspotenzial aus dem Internet und erschwert unter anderem den Missbrauch des Namensdienstes für unerwünschte Kommunikation.

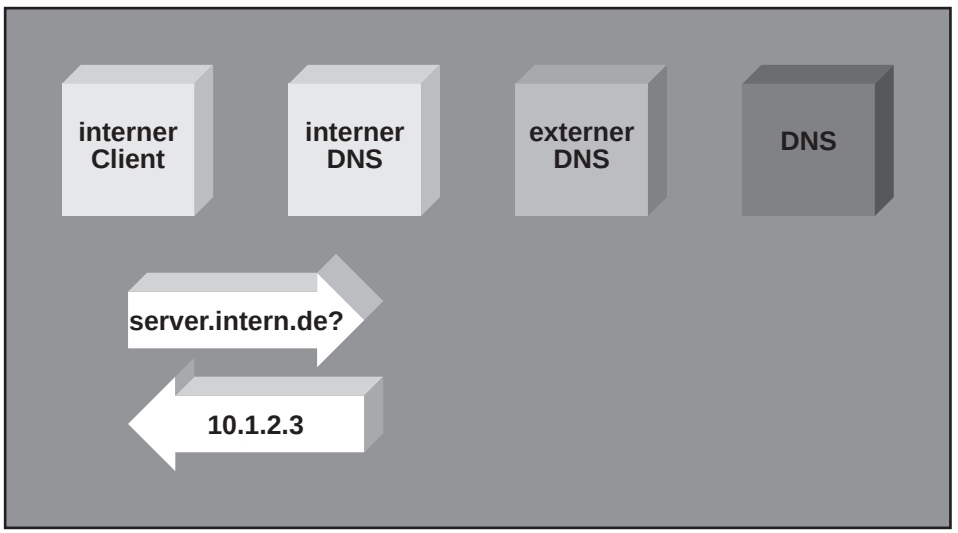


Bild 2 Auflösung von DNS-Anfragen nach internen Zielen

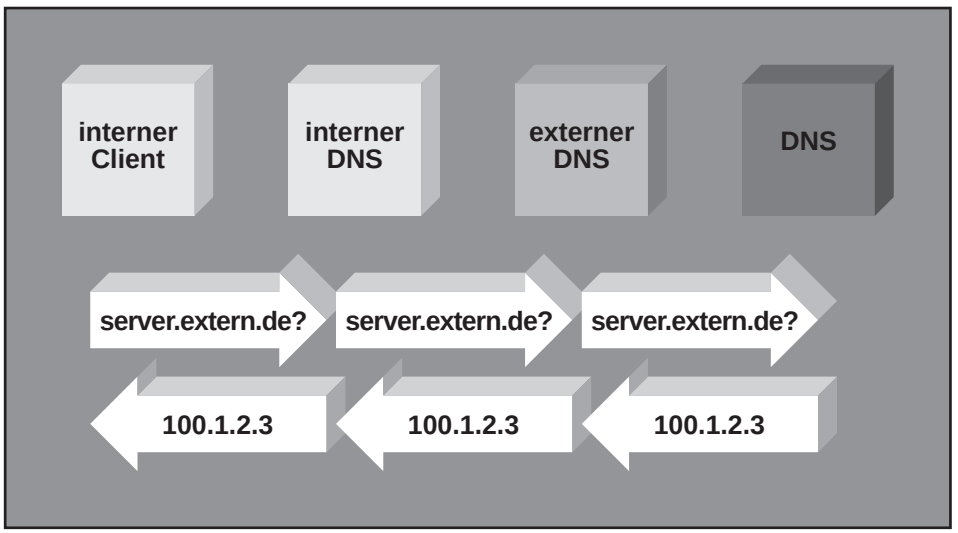
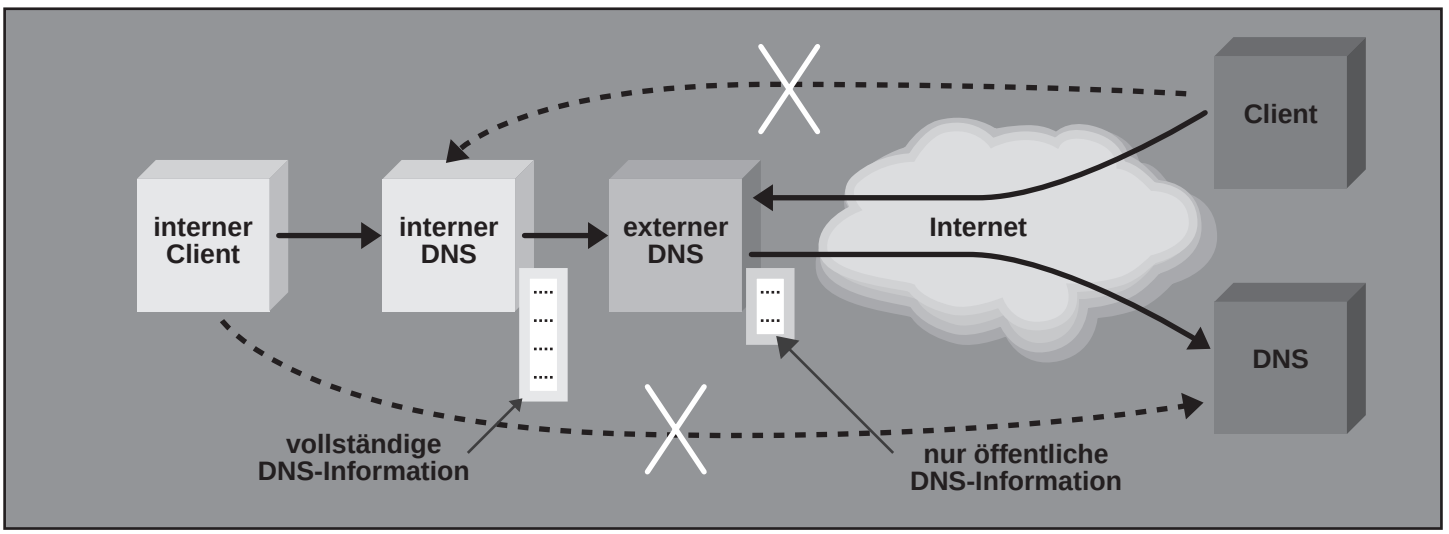


Bild 3 Auflösung von DNS-Anfragen nach externen Zielen

Bild 4 Kaskadierung von DNS-Servern und Split DNS



(Der beliebte Instant Messager ICQ erlaubt es beispielsweise, zur Kommunikation mit der Gegenstelle beliebige Ports zu definieren; hierdurch kann dann etwa auch das DNS-Protokoll als Tunnel für ICQ-Daten missbraucht werden.) Wir benötigen also eine Regel, die die Dienste HTTP und FTP für den internen Proxy frei schaltet, sowie Regeln, die die DNS-Kommunikation zwischen den beteiligten DNS-Servern erlauben.

Bestimmung 2 lässt sich durch eine Authentifizierungsregel, die den Zugriff von außen auf interne Ressourcen auf einen berechtigten Nutzerkreis einschränkt, umsetzen. Alle weiteren derartigen Zugriffe werden durch eine allgemeine "Blockade"-Regel (s.u.) unterbunden.

Je nachdem, welche Rechte man einem solchen Externzugriff einräumt, sollte die Authentifizierung möglichst sicher und zuverlässig gestaltet werden; ansonsten haben Passwort-Cracker oftmals leichtes Spiel. Es versteht sich von selbst, dass man für den Zugriff selbst ein möglichst sicheres Protokoll (z.B. SSH) wählen sollte, das insbesondere die übertragenen Daten durch Verschlüsselung gegen Abhören schützt. Alternativ kann auch über die Einrichtung eines IPSec-basierten Virtuellen Privaten Netzwerks (VPN) nachgedacht werden.

Damit eine Authentifizierung überhaupt möglich ist, muss die Firewall freilich über Eigenschaften verfügen, die über die Funktionalität eines reinen dynamischen Paketfilters hinausgehen: sie muss – zumindest rudimentäre – Application-Proxies zur Verfügung stellen. Was das ist, und was man davon hat, wird noch diskutiert; hier soll zunächst der Hinweis auf die entsprechende Notwendigkeit genügen...

Bestimmung 3 lässt sich auf verschiedene Weise umsetzen; dies hängt stark davon ab, wie das eigene E-Mail-System organisiert ist. Wir werden in diesem Beispiel davon ausgehen, dass ein eigener SMTP-Server betrieben wird; alternativ sind auch z.B. POP3- oder IMAP-Postfächer auf einem Provider-Mail-Server denkbar. Da ein SMTP-Mail-Server zum Empfang von E-Mails für Verbindungen aus dem Internet offen sein muss, Bestimmung 2 solche Zugriffe auf interne Ressourcen jedoch untersagt – ganz abgesehen davon, dass man niemals jemand per SMTP auf das interne Netz zugreifen lassen sollte, ganz egal, wie die Bestimmungen aussehen; dazu ist der Dienst viel zu unsicher – wird in der DMZ ein SMTP-Relay-Server aufgestellt. Dieser dient dazu, E-Mails zwischen dem internen Netz und dem Internet zu vermitteln, so dass direkte Verbindungen zwischen diesen beiden Bereichen nicht notwendig sind.

Dementsprechend benötigen wir Regeln, die die SMTP-Kommunikation des Relay-Servers sowohl mit "drinnen" als auch mit "draußen" ermöglichen.

Bestimmung 4 wird dadurch sicher umgesetzt, dass die öffentlichen Server (Web-Server, FTP-Server, externer DNS-Server) ebenfalls in der DMZ positioniert werden.

Der DNS-Server enthält ausschließlich Informationen über die weiteren aus dem Internet erreichbaren Server (neben den zuvor genannten ist dies vor allem der SMTP-Relay-Server), nicht aber über interne Rechneradressen; dieses Konzept, die DNS-Information in externe und interne Informationen aufzuteilen, um einem Angreifer im Falle eines erfolgreichen Hackens des externen DNS-Servers keine Kenntnisse über das interne Netz zu vermitteln, wird auch als "Split DNS" bezeichnet (vgl. Bild 4): der externe DNS-Server kann nur Anfragen nach öffentlichen Servern positiv beantworten (Bild 5); bei Anfragen nach internen Systemen muss er passen (Bild 6). Im Regelsatz werden Regeln für den Zugriff von außen (HTTP, FTP, DNS) wie auch von innen (ggf. zusätzlich administrativer Zugriff, z.B. zur Pflege der Web-Seiten) benötigt.

Neben den durch die geforderte Funktionalität erzwungenen Regeln sollte in aller Regel eine abschließende "Blockade"-Regel implementiert werden. Aus Sicherheitsaspekten heraus ist diese nicht unbedingt notwendig, da eine Firewall von sich aus jegliche Kommunikation, die nicht durch den Regelsatz ausdrücklich erlaubt wird, unterbindet. Sie tut dies aber heimlich, still und leise – will man über derartige Kommunikationsversuche informiert werden, d.h. sollen solche Aktionen protokolliert werden, muss man eine eigene Blockade-Regel definieren, die eine entsprechende Protokollierung vorsieht.

Bild 5 Auflösung von externen DNS-Anfragen für öffentliche Server

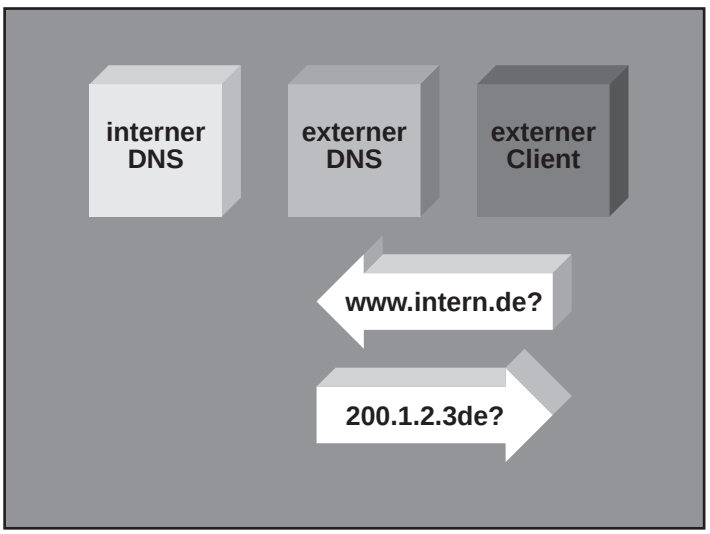
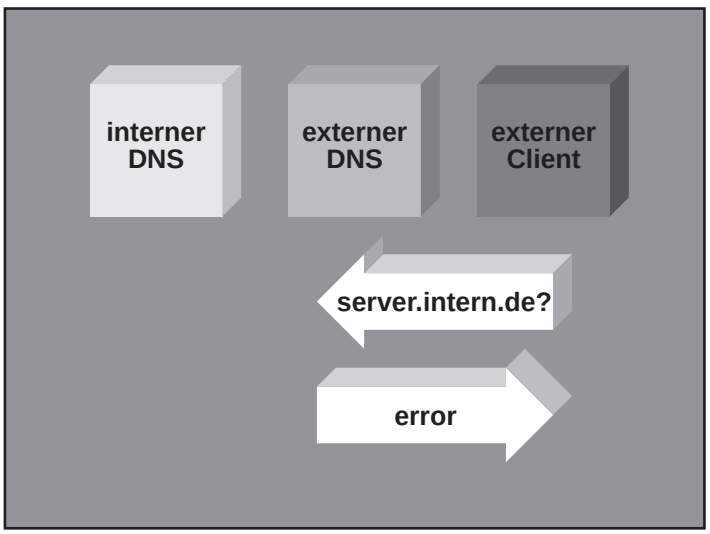


Bild 6 Auflösung von externen DNS-Anfragen für interne Systeme



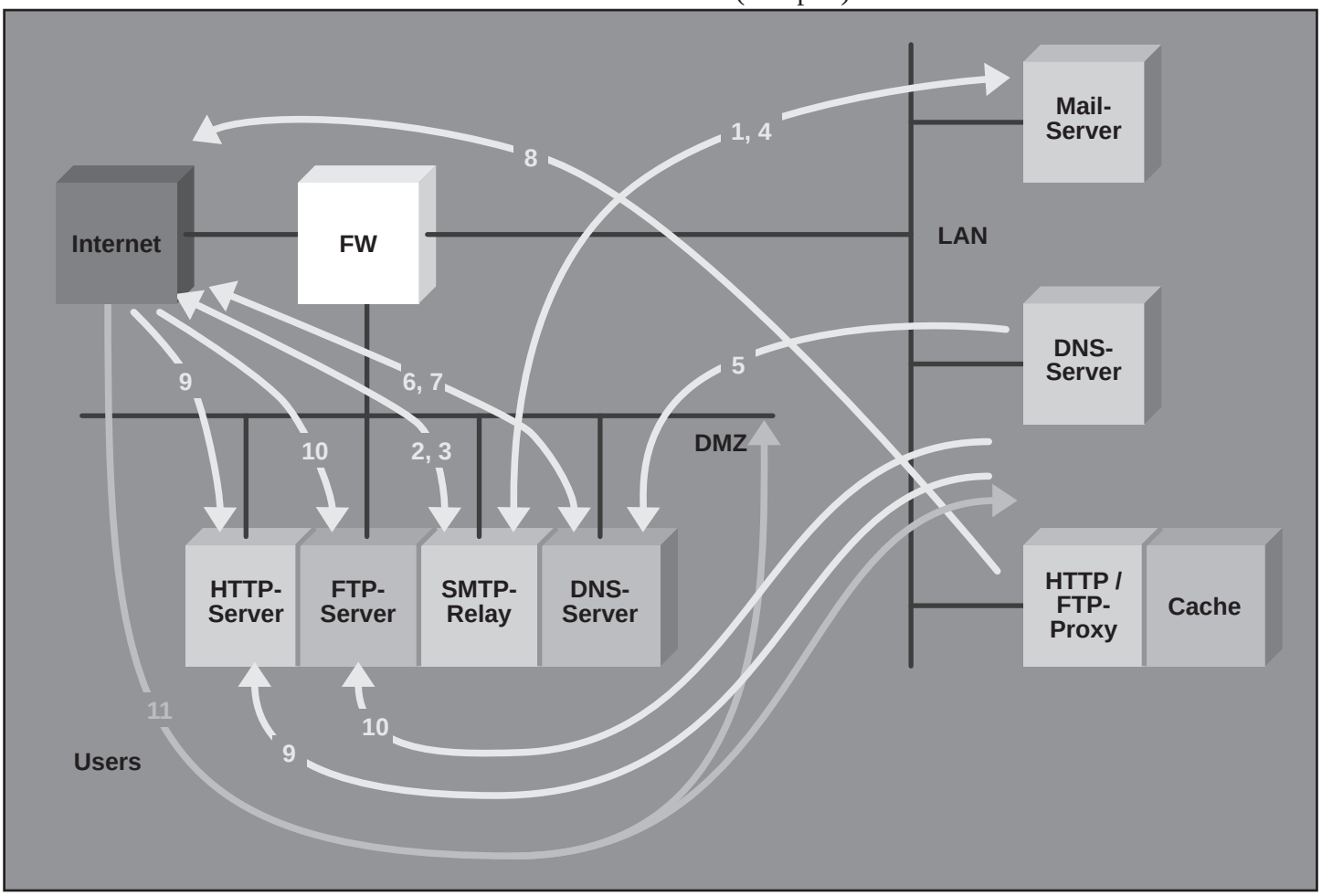
Firewall-Konfiguration nach Maß: Erfahrungswerte aus der Praxis

Da, wie wir bereits gesehen haben, die Reihenfolge der einzelnen Regeln innerhalb des Regelsatzes eine wichtige Rolle spielt, sind diese vor der Implementierung geeignet anzuordnen. Ein geeigneter Beispiel-Regelsatz könnte dann etwa wie folgt aussehen (vgl. Tabelle 1) - die zugehörige Firewall-Architektur wird in Bild 7 illustriert:

Regel	Quelle	Ziel	Quell-Dienst	Ziel-Dienst	Erlaubt?
1	int. SMTP	SMTP-Relay	> 1023	SMTP	ja
2	SMTP-Relay	extern	> 1023	SMTP	ja
3	extern	SMTP-Relay	> 1023	SMTP	ja
4	SMTP-Relay	int. SMTP	> 1023	SMTP	ja
5	int. DNS	ext. DNS	> 1023	DNS	ja
6	ext. DNS	extern	> 1023	DNS	ja
7	extern	ext. DNS	> 1023	DNS	ja
8	HTTP-Proxy	extern	> 1023	HTTP, FTP	ja
9	jeder	HTTP-Server	> 1023	HTTP	ja
10	jeder	FTP-Server	> 1023	FTP	ja
11	Users	jeder	> 1023	SSH	Auth.
12	jeder	jeder	jeder	jeder	nein

Tabelle 1 Firewall-Regelsatz (Beispiel)

Bild 7 Firewall-Architektur (Beispiel)



Firewall-Konfiguration nach Maß: Erfahrungswerte aus der Praxis

Regel 1 erlaubt es dem internen E-Mail-Server, Verbindung über das SMTP mit dem Mail-Relay-Server in der DMZ aufzunehmen; diese Regel wird benötigt, um E-Mails zur Weiterleitung zu versenden.

Regel 2 erlaubt es dem Mail-Relay-Server in der DMZ, Verbindung über das SMTP mit beliebigen Rechnern im Internet aufzunehmen; diese Regel wird benötigt, um die versandten E-Mails weiterzuleiten.

Regel 3 erlaubt es beliebigen Rechnern im Internet, Verbindung über das SMTP mit dem Mail-Relay-Server in der DMZ aufzunehmen; diese Regel wird benötigt, um E-Mails zur Weiterleitung zu empfangen.

Regel 4 erlaubt es dem Mail-Relay-Server in der DMZ, Verbindung über das SMTP mit dem internen E-Mail-Server aufzunehmen; diese Regel wird benötigt, um die empfangenen E-Mails weiterzuleiten.

Regel 5 erlaubt es dem internen DNS-Server, den externen DNS-Server über das DNS-Protokoll zu kontaktieren; diese Regel wird benötigt, um DNS-Anfragen der internen Clients an den externen DNS-Server weiterzuleiten, falls es sich nicht um interne Namen handelt.

Regel 6 erlaubt es dem externen DNS-Server, beliebige Rechner im Internet über das DNS-Protokoll zu kontaktieren; diese Regel wird benötigt, um die DNS-Anfragen der internen Clients sowie des Mail-Relay-Servers an das Internet weiterzuleiten (falls der externe DNS-Server die Antwort nicht weiß).

Regel 7 erlaubt es beliebigen Rechnern im Internet, den externen DNS-Server über das DNS-Protokoll zu kontaktieren; diese Regel wird benötigt, um die Namen der öffentlichen Server einschließlich des Mail-Relay-Servers aus dem Internet auflösen zu können.

Regel 8 erlaubt es dem internen Proxy-Server, Verbindung zu beliebigen Rechnern im Internet über die Protokolle HTTP bzw. FTP aufzunehmen; diese Regel wird benötigt, damit der Zugriff der internen Anwender über den zwischengeschalteten Proxy-Server auf Web-Dienste möglich ist.

Regel 9 und 10 erlauben es beliebigen Rechnern, Verbindung zu den öffentlichen Servern für Web-Dienste über die Protokolle HTTP bzw. FTP aufzunehmen; diese Regeln werden zur Bereitstellung der gewünschten Web-Dienste für die Allgemeinheit (Intra- und Internet) benötigt.

Regel 11 erlaubt es bestimmten Anwendern, beliebige Verbindungen unter Nutzung des Dienstes SSH aufzubauen, sofern sie sich korrekt authentifizieren können; diese Regel wird zur Bereitstellung des authentifizierten Zugriffs auf das geschützte Netzwerk benötigt. Je nach Bedarf können die Kommunikationsziele zusätzlich eingeschränkt werden.

Regel 12 verbietet jegliche Kommunikation; diese Regel wird benötigt, um ggf. eine Protokollierung solcher Datenpakete bzw. Verbindungen zu ermöglichen. Da diese Regel an letzter Stelle steht, wird sie nur dann angewendet, wenn ein Datenpaket bzw. eine Verbindung zu keiner der anderen Regeln passt.

Jetzt legen wir noch fest, bei welchen Regeln wir protokollieren wollen und wie wir blockierte Pakete behandeln – letztere werden üblicherweise heimlich, still und leise verworfen, um erst gar nicht zu verraten, dass hier eine Firewall im Spiel ist; man erreicht dies meistens über eine Option "Drop" oder einen vergleichbaren Parameter. Anschließend sind wir soweit den Regelsatz zu implementieren – jedenfalls fast...

Bevor wir uns an die entsprechende Konfiguration unserer Firewall machen, sind noch zwei weitere Schritte erforderlich. Zum einen muss unser Regelsatz noch um die eine oder andere Regel erweitert werden, die nicht unmittelbar der Umsetzung der Sicherheitsbestimmungen dienen; zum anderen sollte die Firewall selbst vor Implementierung der Regeln optimal gegen Angriffsversuche von Hackern geschützt werden. Letzteres wird auch gerne als "Härtung" bezeichnet und bedeutet nichts anderes, als dass zunächst alle Prozesse und Dienste innerhalb des Firewall-Systems, die nicht unbedingt benötigt werden, deaktiviert werden. Der Grund hierfür ist simpel: je komplexer ein System, desto instabiler arbeitet es und desto größer ist die Wahrscheinlichkeit, dass Sicherheitslücken ein Eindringen durch Angreifer ermöglichen. Eine möglichst robuste Firewall sollte daher nur das unbedingt Allernötigste an Systemkomplexität aufweisen. Nach dieser Entschlackungskur – die ganz nebenbei auch noch die Leistungsfähigkeit des Systems erhöht, indem Ressourcen freigesetzt werden – empfiehlt sich eine Untersuchung des Systems mit einem geeigneten Security-Scanner auf verbliebene Sicherheitsrisiken; diese werden dann sukzessive geschlossen, bis der Scanner weitestgehend Grünes Licht gibt – erst dann ist die Firewall bereit, mit dem eigentlichen Regelsatz versehen zu werden. Diese Härtung empfiehlt sich übrigens bei Firewalls, die nicht als fertige Box (so genannte Appliances), sondern als Software-Lösung konzipiert sind, bereits vor der Installation der Firewall-Software auf der vorgesehenen Betriebssystemplattform.

Die bereits angesprochene Erweiterung des Regelsatzes betrifft mindestens drei funktionale Aspekte:

Erstens ist in den meisten Umgebungen eine ausschließliche Administration der Firewall an der Systemkonsole nicht praktikabel; dort greift man gerne auf entsprechende GUI-Clients zurück, die einen Betrieb der Firewall vom Büroarbeitsplatz aus ermöglichen. In solchen Fällen muss man eine Regel einbauen, die den administrativen Zugriff dieser Clients auf die Firewall gestattet; hierzu wird meist ein entsprechend gesichertes, oftmals proprietäres Protokoll benutzt.

Zweitens neigen manche Systemplattformen trotz der empfohlenen Entschlackung zu einer gewissen Geschwätzigkeit, die man ihnen ohne Funktionsverlust nicht abgewöhnen kann. In solchen Fällen ist der Einbau einer Regel, die diese Kommunikation ohne Protokollierung unterdrückt, dringend anzuraten, da ansonsten die Protokolldateien von derartigen Systemmeldungen, die keinerlei Sicherheitsrelevanz aufweisen, regelrecht überschwemmt werden.

Und schließlich ist es mitunter seitens des Betriebs der Firewall ungünstig, alle nicht zulässigen Datenpakete bzw. Verbindungen über eine einzige abschließende Blockade-Regel zu erfassen: zwar spielt es mit Blick auf das Resultat keine Rolle, welche Regel ein Paket verwirft, solange es nur überhaupt verworfen wird, aber man kann durch gezieltes Einbauen speziell zugeschnittener Regeln dennoch Vorteile erzielen. Derartige Regeln ermöglichen zum einen ein gezieltes Protokollieren und ggf. auch die Auslösung eines Alarms und können zum anderen zur Vermeidung von Fehlkonfigurationen beitragen: Man könnte sich beispielsweise eine spezielle Regel vorstellen, die eine ganz bestimmte, verdächtige Netzwerkadresse komplett blockiert; eine solche Regel sollte am besten ganz nach vorne an den Anfang des Regelsatzes geschoben werden, damit nicht versehentlich eine spätere Regel die diesbezügliche Kommunikation zumindest teilweise doch zulässt...

Da das Stichwort "Alarm" gefallen ist, sei an dieser Stelle eine generelle Empfehlung zum Umgang mit diesem Werkzeug gestattet. Praktisch alle Firewalls ermöglichen die Auslösung solcher Alarme; Ziel eines Alarms ist es, den Administrator der Firewall sofort auf verdächtige Ereignisse aufmerksam zu machen und nicht auf die nachträgliche Feststellung im Rahmen einer generellen Untersuchung der Protokolldateien zu warten, zumal in umfangreichen Protokollen einzelne Ereignisse durchaus schon einmal übersehen werden können (je nach Art der Protokollierung können pro Tag durchaus 100 Mbyte an Protokolldaten anfallen - für eine einfache Textdatei doch ein nicht zu unterschätzender Umfang...). Das Problem hierbei ist nicht das "ob", d.h. ob die Alarmauslösung möglich ist, sondern das "wann", d.h. bei welchen Ereignissen die Firewall sich zu einem Alarm entschließt. Dass dies infolge der fehlenden Fähigkeit gängiger Firewalls, einzelne Ereignisse zueinander in einen Zusammenhang zu stellen und auf dieser Basis Alarme zu generieren, problematisch werden kann, belegt ein weiteres Beispiel auf der Basis einer wahren Begebenheit: Der Autor war einmal an einem Projekt beteiligt, bei dem mehrere Firewalls geplant und eingerichtet werden sollten. Der für die zentrale Administration dieser Firewalls verantwortliche Mitarbeiter bestand trotz eindringlicher Warnung auf einer Benachrichtigung per SMS bei festgestellten Regelverletzungen. Eine kleine Simulation bekehrte ihn dann jedoch schnell: Die testweise Durchführung von 4 Portscans generierte innerhalb kürzester Zeit rund 250.000 (zum Glück nur virtuelle) SMS...

Alarme durch die Firewall sollten daher äußerst sparsam und sehr gezielt eingesetzt werden. Ein Beispiel könnte etwa wie folgt aussehen: Da außer dem Mail-Relay-Server keines der Systeme in der DMZ Verbindung mit dem internen Netz aufnehmen sollte, wäre ein entsprechender Versuch zumindest ein Indiz für einen Hacker-Angriff, z.B. nach Übernahme des Webservers. Da derartiges hoffentlich nur äußerst selten auftritt, könnte man in diesem Fall eine spezielle Regel einfügen, die jeglichen Datenversand aus der DMZ an das interne Netz verbietet und außerdem einen Alarm auslöst; diese Regel muss natürlich soweit nach hinten innerhalb des Regelsatzes geschoben werden, dass die E-Mail-Weiterleitung noch möglich ist – in unserem Beispiel also etwa hinter Regel 4.

Der entsprechend ergänzte Regelsatz kann nunmehr implementiert werden. Bei dieser Implementierung sollte auf sinnvolle Dokumentation allergrößter Wert gelegt werden, damit Sinn und Zweck der Regeln auch im Nachhinein und für nicht mit der ursprünglichen Regelerstellung befasste Administratoren noch nachvollziehbar ist.

Ein Wort zu Application Proxies

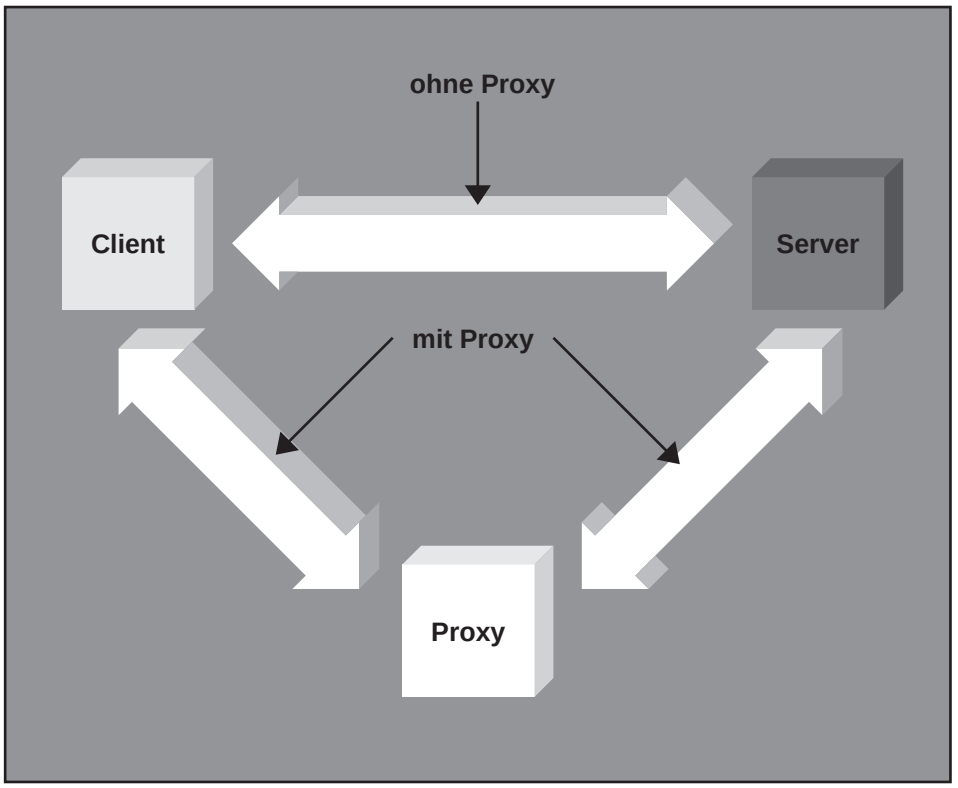
Neben dem beschrieben (dynamischen) Paketfilter gibt es einen weiteren Typ von Firewalls: so genannte Application Gateways. Diese sind - nicht zuletzt aufgrund der höheren Kosten, die ihre Ursache sowohl im höheren Entwicklungsaufwand als auch in den weitergehenden Anforderungen an die Leistungsfähigkeit der Systemplattform haben – deutlich seltener anzutreffen; gleichwohl stellen sie gewissermaßen den Stammvater aller Firewalls dar: die ersten Firewall-Ansätze basierten auf dem Einsatz entsprechend abgesicherter Application Proxies.

Ein solcher (Application) Proxy fungiert als Mittler zwischen Netzwerken, indem er sich auf der Anwendungsebene in die Kommunikation zwischen Client und Server "einklinkt" – dies kann sowohl bewusst, d.h. mit Kenntnis des Clients bzw. Anwenders, als auch unbewusst ("transparent") geschehen. In beiden Fällen kommunizieren Client und Server nicht direkt miteinander, sondern jeweils mit dem Proxy, der die Anwendungsdaten entsprechend weiterleitet (Bild 8).

Dabei ist es wichtig zu wissen, dass ein vollwertiger Proxy das Anwendungsprotokoll ausführt, d.h. die entsprechenden Kommandos ausführt und die Daten entsprechend manipuliert. Ein einfaches Beispiel für einen solchen Proxy ist ein Web-Proxy (s.o.), der die HTTP-Requests der Clients entgegennimmt und an den tatsächlichen Server weiterleitet, sofern er die Anforderung nicht selbst aus seinem Cache bedienen kann. Proxy-basierte Firewalls besitzen, da sie das Anwendungsprotokoll ausführen, Filterfunktionen, die z.T. weit über die von Paketfiltern hinausgehen; insbesondere kann etwa der zulässige Befehlssatz des Anwendungsprotokolls eingeschränkt oder die Ziel-URL in Requests auf illegale Inhalte hin untersucht werden.

Ein weiteres Anwendungsfeld ist die Filterung bestimmter aktiver Inhalte (sog. Mobile Code) wie etwa Java Applets, Java Script oder ActiveX. Allerdings kann die Firewall an dieser Stelle lediglich die Existenz solcher Inhalte verifizieren und in Abhängigkeit von ihrer Policy diese Inhalte entweder sperren oder passieren lassen; für eine Entscheidung, inwieweit dieser Code eventuell Schaden anrichten kann, weil er etwa Viren, Würmer oder Trojaner enthält, sind Firewalls nicht ausgerüstet.

Bild 8 Funktionsweise eines Proxy



Dies muss über separate Scanner erfolgen, die z.B. auf der Basis des Sandbox-Verfahrens den Code auf "Ungefährlichkeit" testen. In den meisten Umgebungen empfiehlt es sich aus Performance-Gründen, solche Scans bzw. Tests dezentral auf den Clients durchzuführen; eine vollständige Sperrung durch die Firewall ist jedenfalls in den meisten Fällen nicht mehr praktikabel, da sonst mehr und mehr Websites nicht mehr vollständig dargestellt werden können. Hier sollte u.a. auch auf eine möglichst robuste und sichere Konfiguration der Browser geachtet werden...

Die Ausführung des Anwendungsprotokolls erhöht aber nicht nur die Leistungsfähigkeit der Firewall als Schutzmechanismus, sondern bringt auch gewisse Nachteile mit sich; so sind Proxy-Firewalls in aller Regel hinsichtlich des Datendurchsatzes gegenüber Paketfiltern eingeschränkt und unterstützen u.U. nicht alle Anwendungen; insbesondere seltene Anwendungen oder gar Eigenentwicklungen werden meist nicht bedient. Hier behilft man sich dann mit so genannten "Generischen Proxies", die der Firewall-Administrator selbst definieren kann; allerdings führen diese eben nicht das Anwendungsprotokoll aus, sondern klinken sich lediglich auf der Transportebene in die Kommunikation ein, d.h. die direkte Verbindung zwischen Client und Server wird unterbrochen, aber die Daten des Anwendungsprotokolls werden ohne Kontrolle oder gar Beeinflussung durch die Firewall weitergeleitet.

Je nach Implementierung und Rahmenbedingungen kann allerdings auch ein vollwertiger Application Proxy nicht alle Daten inspizieren: wird eine Anwendung auf Basis eines verschlüsselten Protokolls (z.B. HTTPS) eingesetzt, so kann die Firewall die Anwendungsdaten nur dann kontrollieren, wenn sie sowohl für den Client als auch für den Server die jeweiligen verschlüsselten (z.B. SSL-) Tunnel terminiert. Diese Vorgehensweise, sofern sie vom Firewall-Proxy unterstützt wird, bedarf aber des Einverständnisses von Client und Server. Akzeptiert der Client z.B. bei einer SSL-geschützten Verbindung das Zertifikat der Firewall nicht (etwa, weil es ein spezieller Client ist, der nur das Zertifikat eines speziellen Servers kennt und akzeptiert), so ist eine Tunnelterminierung und damit verbunden eine Entschlüsselung der Daten nicht möglich...

Proxies oder vergleichbare Mechanismen werden von Firewalls auch immer dann benötigt, wenn eine Authentifizierung von Benutzern stattfinden soll. Der Proxy ermöglicht den Austausch der notwendigen Identifizierungsdaten mit dem Client. Dazu reicht es allerdings, dass er beim Verbindungsaufbau einige rudimentäre Schritte des Anwendungsprotokolls ausführen kann. Nach erfolgter Authentifizierung ist die Protokollausführung nicht mehr notwendig. Derartig eingeschränkte Proxies verwendet z.B. die Cisco PIX Firewall (unter der Bezeichnung "Cut Through Proxy"). Ein weiteres Beispiel für eingeschränkte Proxies liefert die Checkpoint Firewall-1: ihre so genannten "Security Server" führen zwar – sofern sie nicht ausdrücklich nur zur Authentifizierung eingesetzt werden – stets das Anwendungsprotokoll aus, bieten aber dennoch nicht alle Funktionen eines vollwertigen Proxies (z.B. ist der SMTP-Security Server nicht in der Lage, DNS-Anfragen zu tätigen...).

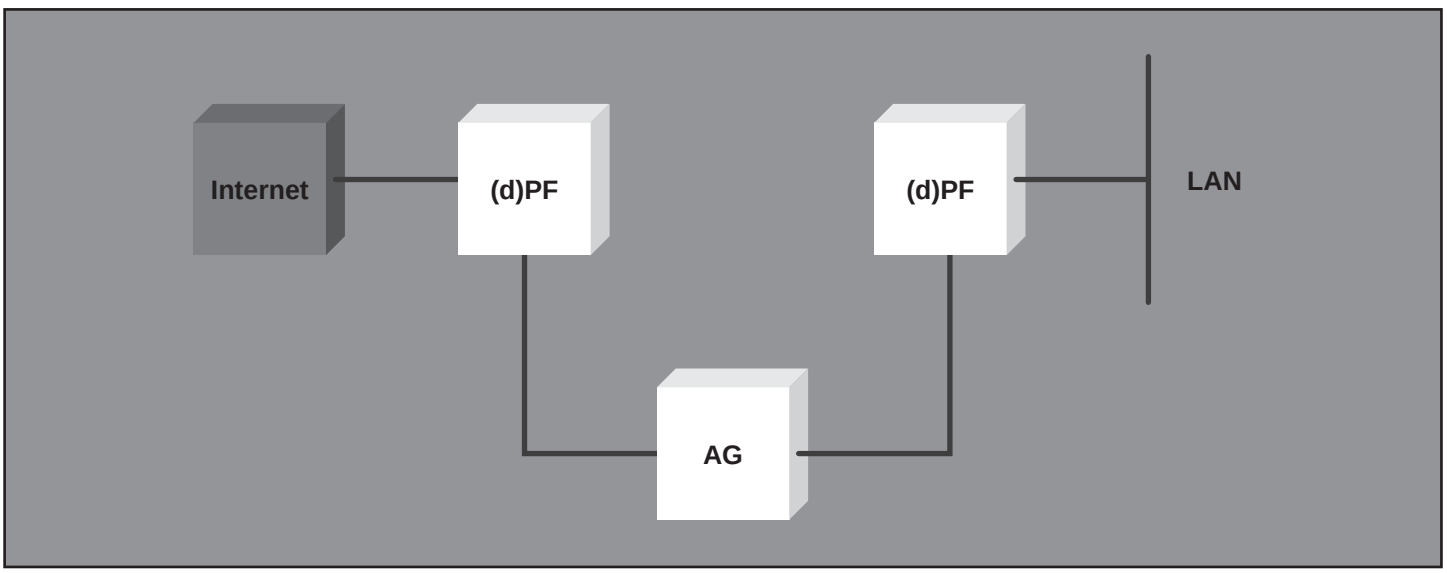
Wann sollte man nun Proxy-Firewalls einsetzen?

Sieht man von der Authentifizierungsthematik ab, so kommen Application Gateways in der Regel dann in Betracht, wenn entweder

- die Anforderungen an die Sicherheit generell so hoch sind, dass sie eine Filterung auf Anwendungsebene sinnvoll erscheinen lassen,
- oder bestimmte gewünschte bzw. erforderliche Filterfunktionen ausschließlich von Application Proxies zur Verfügung gestellt werden können.

In beiden Fällen ist darüber hinaus Voraussetzung, dass die geringere Performance und die höheren Kosten in Kauf genommen werden können. Ob die Proxy-Funktionalität dabei besser innerhalb der eigentlichen Firewall, d.h. in Form einer Kombi-Lösung aus Paketfilter und Application Proxy, oder durch ein separates System realisiert wird, hängt vom konkreten Szenario, den Sicherheits- und Funktionalitätsanforderungen sowie den Möglichkeiten der einzusetzenden Firewall-Produkte ab. Optimale Sicherheit (u.a. auch nach Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik, BSI) bietet dabei eine Kaskadierung von Paketfiltern und Application Gateway (Bild 9), allerdings ist eine solche Lösung auch recht aufwändig und kostenträchtig.

Bild 9 Mehrstufige Firewall nach BSI-Empfehlung



Tuning gefällig?

Die erstellten Regeln stellen die funktionale Umsetzung der Sicherheitsbestimmungen sicher. Aus diesem Blickwinkel betrachtet, gibt es zunächst nichts mehr zu ändern, allerdings kann man durch kleine Optimierungen noch ein wenig mehr an Leistung aus der Firewall und dem Internetzugang herausholen. Freilich sollte man an die durch die nachfolgend beschriebenen oder andere, vergleichbare Maßnahmen erzielbaren Effekte keine übersteigerten Erwartungen stellen. In den meisten Fällen wird die Gesamtperformance einer Internetanbindung nicht durch die Firewall maßgeblich bestimmt, sondern durch die Bandbreite des Internet-Access: moderne Systeme auf zeitgemäßen Hardware-Plattformen sind meistens nur zu einem äußerst moderaten Teil ihrer Gesamtkapazität ausgelastet, so dass manche Performance-Effekte zwar messbar, aber für den Anwender kaum zu spüren sein dürften. Demgegenüber sind breitbandige Anbindungen an den Provider hierzulande immer noch vergleichsweise teuer und die verfügbare Bandbreite daher in den allermeisten Fällen eher knapp bemessen.

Ein Ansatzpunkt zur Optimierung ist einmal mehr die Reihenfolge der Regeln innerhalb des Regelsatzes. Da die Firewall für jedes Datenpaket den gesamten Regelsatz nach einer passenden Regel absuchen muss, lässt sich die Suchzeit und damit die Verzögerung, die der Transport des betroffenen Datenpakets erfährt, dadurch beeinflussen, dass die zutreffende Regel möglichst weit vorne im Regelsatz platziert wird. Da man natürlich nicht für alle Datenpakete die jeweils passende Regel an den Anfang des Regelsatzes stellen kann, muss man die Optimierung des Gesamtdurchsatzes dadurch vornehmen, dass Regeln, die häufiger zutreffen - weil die korrespondierenden Datenpakete einen größeren Anteil am Gesamtpaketaufkommen haben - als andere, entsprechend weiter nach vorne im Regelsatz gestellt werden.

Aber Achtung: nicht in allen Fällen führt diese Vorgehensweise auch zu entsprechenden Leistungssteigerungen; je nach Implementierung einer Firewall wird für bestehende Kommunikationsbeziehungen u.U. gar nicht mehr die gesamte Regelbasis untersucht, sondern nur noch eine relevante Teilmenge, so dass sich der Reihenfolge-Effekt ganz unterschiedlich auswirken kann. Dennoch: einen Versuch ist es sicherlich allemal wert ...

Ein weiteres Beispiel für eine Verbesserung der Gesamtperformance ist die Unterdrückung unerwünschten (weil unproduktiven) Datenverkehrs. Hierunter fallen z.B. Kommunikationsbeziehungen von Instant Messaging Systemen (ICQ, AIM, etc.), die nicht nur Arbeitszeit kosten sondern auch Bandbreite, aber auch die allenthalben anzutreffenden Werbebanner. Diese kann man entweder über entsprechende proxygestützte Filtermechanismen oder über Sperrung zumindest der bekanntesten diesbezüglichen Server (z.B. Doubleclick) ausblenden. Aber auch hier heißt es "aufgepasst": Wenn Sie, wie allgemein üblich, blockierten Datenverkehr "droppen", d.h. kommentarlos verwerfen, so wartet der Client jedes Mal bis zum Ablaufen eines entsprechenden Timers auf das Zustandekommen der Verbindung zum blockierten Server. Somit profitiert zwar die Allgemeinheit von der eingesparten Bandbreite aber die betroffenen Clients warten und warten und warten... Deshalb sollten Sie für solche Aktionen (sofern Ihre Firewall dies anbietet) statt der Aktion "Drop" die Aktion "Reject" wählen; in diesem Fall erhält der Absender des verworfenen Pakets eine Nachricht, dass das Ziel nicht erreichbar ist, und kann unmittelbar weiterarbeiten...

So -
das war's...
Oder etwa doch nicht?

Nicht selten lehnt sich der Verantwortliche nach abgeschlossener Implementierung und Inbetriebnahme entspannt zurück und überlässt die Firewall ihrem Schicksal; das System wird bestenfalls wie jedes andere Server-System betreut, d.h. es wird bei Bedarf herunter- und wieder hochgefahren und unterliegt möglicherweise einer automatisierten Datensicherung. Doch Vorsicht: sich so zu verhalten ist nicht ungefährlich. Ein Firewall-System verlangt nach einem kontinuierlichen Betrieb und einer gewissen Überwachung, ansonsten wiegt man sich womöglich in trügerischer Sicherheit. Immerhin entwickelt die Hackergemeinde kontinuierlich neue Angriffsmethoden, die früher oder später eine Anpassung der vorhandenen Firewall an das gestiegene Bedrohungspotenzial erforderlich machen können, oder, im schlimmsten Fall, sogar zu einem geglückten Einbruch in das scheinbar geschützte Netzwerk führen können. Ohne regelmäßige Beobachtung bleiben solche Ereignisse meist lange Zeit unentdeckt und können zu immensem Schadensausmaß führen. Wohlgemerkt: eine Überwachung der Firewall, d.h. mindestens eine regelmäßige Sichtung der Protokolldateien auf Auffälligkeiten, gibt keine Garantie gegen erfolgreiches Eindringen, aber ohne derartige Maßnahmen ist die Gefahr für Hacker, entdeckt zu werden, deutlich geringer - meist wird man erst dann aufmerksam, wenn der eingetretene Schaden unübersehbar geworden ist.

Mitunter, und diese Anekdote soll denn auch den Schlusspunkt setzen, setzen Netzwerk-Verantwortliche gar Firewalls ein, die überhaupt niemand mehr bedienen kann; im vorliegenden, realen Fall wusste man weder, was genau die Firewall tut (Dokumentation und Handbuch: Fehlanzeige), noch, warum... Ein Gutes hatte das Ganze freilich: Da die neu erarbeiteten Sicherheitsbestimmungen mangels Administrationskenntnissen für das obendrein recht exotische Produkt nicht implementiert werden konnten, wird eine komplett neue Lösung aufgebaut; es steht zu hoffen, dass man diesmal nicht die gleichen Fehler macht wie beim ersten Versuch...

Abk.-Tabelle

BSI	**Bundesamt für Sicherheit in der Informationstechnik**
DMZ	**Demilitarisierte Zone**
DNS	**Domain Name Service**
FTP	**File Transfer Protocol**
LAN	**Local Area Network**
SMTP	**Simple Mail Transfer Protocol**
VPN	**Virtual Private Network**

Aktueller Kongress

Security-Event des Jahres: Netzwerk Sicherheits-Forum 2003

Vom 19. bis 22. Mai 2003 veranstaltet die ComConsult Akademie zusammen mit der GAI NetConsult im Maritim Königswinter das diesjährige "Netzwerk Sicherheits-Forum". Geleitet und moderiert wird die Veranstaltung wie in den letzten Jahren von Dipl.-Inform. Detlef Weidenhammer (GAI NetConsult).

Das diesjährige Netzwerk Sicherheits-Forum beginnt am ersten Tag mit einem einführenden (optionalen) Tutorium. Hier wird neben dem notwendigen Basiswissen auch ein umfassender Überblick zum aktuellen Stand der IT-Security gegeben. Darauf aufbauend werden dann die Referenten an den folgenden drei Tagen inhaltlich stärker in die Tiefe gehen. Neben der Behandlung von aktuellen Sicherheitsproblemen und -techniken werden insbesondere praktische Erkenntnisse vermittelt und reale Lösungen vorgestellt. Erfahrungsberichte von kompetenten Anwendern zeigen auf, mit welchen Problemen bei der Durchführung von Sicherheitsprojekten zu rechnen ist und wie man ihnen begegnet.

Aktuelle Informationen für Techniker und Entscheider

Fachvorträge zu aktuellen und neuen Sicherheitsthemenn

Tutorium über Grundlagen und Stand der IT-Security

Best Practice: Direkt umsetzbare Praxisempfehlungen

Workshops mit Produktvergleichen und Fallstudien

Ein ganzer Tag wird Praxis-Workshops gewidmet sein, die in parallelen Sessions angeboten werden, um den Teilnehmern eine breite aber auch individuelle Auswahl zu ermöglichen. Neben moderierten Produktvergleichen und Arbeitsgruppen zum Aufbau von Policies und Konzepten werden auch wieder interessante Life-Hacks vorgeführt. "Best Practices" geben in kompakter Form Empfehlungen zu weit verbreiteten Problembereichen.

Die überaus große Beteiligung und die positive Resonanz auf die letzten Foren zeigt uns, dass wir mit der Auswahl der Themen das Interesse der Teilnehmer gefunden haben. Damit ist das "Netzwerk Sicherheits-Forum" für jeden Sicherheitsverantwortlichen und -interessierten zu einer unverzichtbaren Plattform für aktuellste Informationen, Produktvergleiche und Fachdiskussionen geworden.

Netzwerk Sicherheits-Forum 2003 – Die Themen:

Risk Management und Business Continuity
- KonTraG-Anforderungen an ein Risk Management System
- Rechtliche Probleme und Haftungsfragen
- Etablierung einer Notfallorganisation
- Notfalltests, Wartung, Krisenmanagement

Auditierung und Zertifizierung
- Zielsetzung
- Organisatorische Vorbereitungen
- Erfahrungen mit dem BSI IT-Grundschutz Zertifikat
- Prüfungen nach BS7799

Wirtschaftlichkeit und IT-Security
- Kennzahlenermittlung
- Bewertung von Personal- und Technikeinsatz
- ROSI Return on Security Investment
- Einsatz von Risk Scorecards

Sicherer Einsatz von E-Mail
- Risiken beim Einsatz von E-Mail
- Sicherer Betrieb von E-Mail Servern
- Bewertung und Vergleich von Verschlüsselungslösungen
- Rechtliche Aspekte

Sicherung einer IBM Host-Umgebung
- Angriffsmöglichkeiten bei OS/390 und Linux
- Ergebnisse eines Penetrationstests
- Gegenmaßnahmen auf dem Host
- Sichere Host-Einbindung in ein LAN

Sicherheit im WLAN
- Aktuelles zur Standardisierung
- Sicherung von Private und Public WLANs
- Prüfungen mit WLAN Security-Scannern
- Produktvergleiche

Kommunikationssicherheit im LAN
- Betrieb von DNS, DHCP, SSL, SSH
- Sniffing auch in geswitchten Netzen
- Spoofing und MitM-Angriffe, Denial-of-Service Angriffe

RAS und VPN
- VPN als RAS-Lösung
- LAN-LAN und Client-LAN Kopplungen
- Anforderungen an VPN-Provider
- Sicherheitsrisiko Endgerät

Neue Bedrohungen der Content-Security
- Gefahren durch active contents
- Port-80 Problematik
- Aufbau einer mehrstufigen Schutztopologie
- Zentrales Management für AV-Lösungen

Weitere Vortragsthemen
- Sichere Administration im LAN
- Schutzmaßnahmen für mobile Systeme
- Rollen- und Berechtigungskonzepte
- Management von Intrusion Detection Systemen
- Einsatzerfahrungen mit PKI-Lösungen
- Drohende Gefahren durch Web-Services
- Sicherung von Web-Applikationen
- Bedrohung durch Wirtschaftsspionage

Praxis-Workshops
- Moderierte Produktvergleiche
- Live Hacking und Gegenmaßnahmen
- Aufbau von Security-Policy und -Richtlinien

Best Practices zu den Themen
- Konfiguration des Internet-Explorers, Konfiguration von Windows
- Aufbau einer Netzsicherung mit Firewall, DMZ, Security-Gateways

Die Veranstalter behalten sich Änderungen im Programm vor.

Anzeige

10 % Frühbucherrabatt bis 31.03.03

Netzwerk Sicherheits-Forum 2003

19.05. - 22.05.03 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das Netzwerk Sicherheits-Forum 2002 bis zum 15.04.2002 für eine rabattierte Teilnahmegebühr an. In diesem Jahr besteht auch erstmals die Möglichkeit, die Veranstaltung 3-tägig oder 4-tägig (mit Tutorium am ersten Tag) zu buchen:

4 Tage Netzwerk Sicherheits-Forum 2003 vom 19.05. -22.05.03 mit Tutorium
zum Preis bei Buchung bis 31.03.03 von € 1.610,--
statt regulär € 1.790,-- zzgl. MwSt.

3 Tage Netzwerk Sicherheits-Forum 2003 vom 20.05. - 22.05.03 ohne Tutorium
zum Preis bei Buchung bis 31.03.03 von € 1.430.--
statt regulär € 1.590,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk Sicherheits-Forum 2002

Ich melde mich an für das
Netzwerk Sicherheits-Forum 2003

☐ **vom 19.05. - 22.05.03 mit Tutorium**
zum Preis von € 1.610,-- zzgl. MwSt.*

☐ **vom 20.05. - 22.05.03 ohne Tutorium**
zum Preis von € 1.430,-- zzgl. MwSt.*

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____

*Frühbucherpreise gültig bis 31.03.03

Buchen Sie über unsere Web Site:
www.comconsult-akademie.de

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

.NET

Die neuen .NET-Seminare des Competence Center Backoffice

.NET-Server 2003 – plan build & run

Microsoft wird mit der Einführung der Windows .NET-Server 2003-Varianten auch eine Weiterentwicklung des Active Directory und des IP-Management implementieren.

Die ComConsult Akademie hat ihre erfolgreiche Seminarreihe "Windows Active Directory - plan, build, run" vollständig aktualisiert und präsentiert ab März 2003 den Nachfolger ".NET-Server 2003 – plan, build & run" mit dem 5 tägigen Seminar ".NET-Server 2003 – plan: Windows Active Directory und IP Management" und der 4 tägigen Fortsetzung ".NET-Server 2003 – build & run: Windows Active Directory".

Die Seminarreihe richtet sich an Planer, Betreiber und Administratoren, die Windows .NET Server 2003 (oder Windows 2000) Active Directory einsetzen wollen.

Das Seminar ".NET-Server 2003 – plan" liefert neben den erforderlichen Grundlagen insbesondere die Kenntnisse zum Design dieser neuen Landschaft. Besonders ist zu erwähnen, dass diese Kenntnisse auch ihre Gültigkeit für das Design einer Windows 2000 Umgebung haben, da die Weiterentwicklung mit .NET berücksichtigt wird und somit Planungsfehler vermieden werden können. Unterstützt durch Live-Demonstrationen und Übungsbeispiele lernen die Teilnehmer auch, richtige Entscheidungen für ihre eigene Umgebung zu treffen.

Ebenfalls befasst sich das Seminar mit der Koexistenz des Active Directory mit anderen Verzeichnisdiensten und Repositories, eine infrastrukturelle Basis zur Senkung der TCO im Unternehmen. Die im Seminar erarbeiteten Vor- und Nachteile im Bereich des IP-Managements und des Active Directory bilden dann das Fundament für die abschließend betrachtete Projektplanung.

Die Teilnehmer lernen

- komprimiert die Grundlagen des Active Directory
- detailliert das logische Design des Active Directory (Forest, Tree, Domain, OU ...) und deren Gestaltungsmöglichkeiten

- detailliert das physikalische Design des Active Directory (Site, Site-Links ...) und deren Anforderungen
- die Grundlagen zum erforderlichen IP-Management
- detailliert die IP-Management-Serverimplementierungen aus Windows .NET-Server 2003 und Windows 2000
- das Zusammenspiel zwischen DNS und Active Directory, auch mit anderen DNS-Implementierungen, wie beispielsweise BIND
- die Koexistenz des Active Directory mit anderen Verzeichnisdiensten und Repositories
- Active Directory zu projektieren

Dieses Seminar ist auch für Entscheider geeignet, die fundierte Kenntnisse erlangen möchten.

Die Referenten sind die jeweiligen Consulter des Competence Center Backoffice der ComConsult Beratung und Planung GmbH für die verschiedenen Spezialthemen: Competence Center Leiter Markus Holländer für AD im Projekt und AD mit anderen Repositories, Dipl.-Inform. Michael van Laak für AD Grundlagen und logisches Design, Frank Neunzig für physikalisches Design AD und Dipl.-Ing. Lars Kuhl für IP-Management.

Nach der Vermittlung dieser Grundlagen im Seminar ".NET-Server 2003 – plan" befasst sich das 4-tägige Praxisseminar " .NET-Server 2003 – build & run" schwerpunktmäßig mit der Migration von Windows NT 4.0 und Windows 2000 zum Windows .NET Server 2003 Active Directory und dem anschließenden Betrieb dieser Landschaft.

Die Teilnehmerzahl dieses Praxisseminars ist auf 12 Personen beschränkt.

Die Teilnehmer werden selbst in einem Testnetz Migrationen durchführen und verschiedene Tools live am Rechner testen können. Auch werden verschiedene Konstellationen vor- und nachgestellt und klare Empfehlungen ausgesprochen.

Die Teilnehmer lernen und testen in diesem Seminar

- verschiedene Migrationsstrategien (Inplace-Upgrade, Parallel-Migration, inkl. Aufbau einer Testumgebung, Hybride Migrationsvarianten) und deren Vor-/Nachteile,
- Tools, die bei der Migration erforderlich sind
- diverse Zusatzansätze, die oft einen besseren Weg darstellen
- verschiedene Verwaltungsprogramme für eine effiziente Administration von Windows .NET-Server 2003, den .NET-Server Tools, den Support Tools, den Ressource Tools und Tools von Drittherstellern

Neben den theoretischen Vortrags- und Diskussionsteilen steht die praktische Durchführung durch die Teilnehmer im Rahmen verschiedener Szenarien im Vordergrund des Seminars. Dies hat zur Folge, dass die Teilnehmer u.a. die Empfehlungen, die im Rahmen des Seminars ausgesprochen werden, leicht nachvollziehen können und verschiedene Konstellationen besser einschätzen können.

Die Referenten des ".NET Server 2003 – build & run"-Seminars sind Markus Holländer und Dipl.-Inform. Michael van Laak, die Spezialisten mit mehrjähriger Konzipierungs-, Betriebs- und Seminarerfahrung, die schon die erfolgreichen Vorgängerseminare "Migration zu Windows 2000 Active Directory" und "Betrieb von Windows 2000 Active Directory" durchgeführt haben.

Beide Referenten werden an allen Tagen anwesend sein, damit auch eine bestmögliche individuelle Betreuung der Teilnehmer an ihren Testrechnern ermöglicht wird.

.NET E2K (Exchange Server)

Mit der Einführung von Exchange 2000 Server (E2K) ändern sich die Konfiguration und die damit verbundenen Möglichkeiten gravierend. Durch die Notwendigkeit, Active Directory einzusetzen, ergeben sich erhebliche Abhängigkeiten zwischen AD-Gesamtdesign und Mail-Konfiguration.

Dazu müssen den Designern des Active-Directory die Anforderungen der Mail-Konfiguration bekannt sein und umgekehrt müssen die Betreiber des Exchange-Servers ein Grundverständnis der Möglichkeiten des Active Directory entwickeln. Nur so können schwere Fehler im Design vermieden werden und die Betriebspotentiale von Active Directory voll genutzt werden. Exchange 2000 Server ist das erste Backoffice-Produkt, welches sich komplett in das Active Directory einfügt und die Web Storage Technologie nutzt. Damit verlässt Exchange 2000 Server das bisherige Design und die entsprechenden Technologien von Exchange 5.5 völlig.

Eine Koexistenz von Exchange 5.5 mit Exchange 2000 in einem Windows 2000 / .NET-Netzwerk ist möglich, jedoch ist das Design und auch das Handling des SMTP-basierten Messaging-Servers von Microsoft in vieler Hinsicht einfacher und ausbaufähiger geworden. Viele Firmen, die zur Zeit ihre Konzepte zur Migration von NT / Exchange 5.5 entwickeln, müssen sich fragen, inwiefern nicht der direkte Umstieg nach .NET 2003 Server und Exchange 2003 Server sinnvoll ist. Die Erscheinungstermine sind jeweils für Frühjahr und Sommer 2003 angekündigt.

Das 4-tägige Seminar ".NET Exchange Server" soll helfen, eine kompetente Entscheidung zu finden.

Das Seminar befasst sich mit der Implementierung von E2K im Kontext des Windows 2000 - Active Directory Designs. Es werden Grundkenntnisse über Active Directory und Messaging vorausgesetzt. Im Seminar erhalten die Teilnehmer zudem Einblicke in die neuen Architekturen von Microsoft .NET 2003 Server und Microsoft Exchange 2003 Server (Codename "Titanium"). Beide Produkte werden im Laufe des Jahres 2003 herausgegeben werden. Damit stellt sich die Frage für Migrationsprojekte, ob diese Produkte schon einbezogen werden sollten. Zur Sprache kommen im Seminar auch die im Exchange 2003 Server "on board" vorhandenen Softwaremodule Microsoft Operation Manager (MOM), Microsoft Mobile Information

Server (MIS), Microsoft Metadirectory Service (MMS). In den Vorträgen werden die unterschiedlichen Leistungsmerkmale, Features und Funktionen vorgestellt. Dabei werden viele Bestandteile live oder durch Videoaufnahmen demonstriert. Vorträge, Bild- und Videodarstellungen stehen in den Teilnehmerunterlagen zur Verfügung.

Das Seminar richtet sich an Planer, Betreiber und Administratoren, die Microsoft Backoffice-Produktlinie im Unternehmensnetz einsetzen wollen.

Die Teilnehmer lernen

- Aufbau einer Messaging-Infrastruktur unter NT, Windows 2000 und .NET 2003 Server
- Einsatzmöglichkeiten von Exchange 5.5, Exchange 2000 und Exchange 2003 Servern
- Implementierung von Exchange Server in das Active Directory-Konzept Ihres Netzwerkes
- Architektur von Exchange Server bezüglich Speicherung, Messageflow, Verwaltung und Sicherheit
- Clientzugriffe im Internet und über das Internet
- Upgrade und Migration
- Connectivity mit anderen Microsoft Backoffice Produkten

Der Referent ist Hans Willi Kremer von der ComConsult Beratung und Planung

.NET IIS (Internet Information Server)

Der IIS erfreut sich wachsender Bedeutung im MS Backoffice-Segment. Er ist vom reinen Webserver zum allgegenwärtigen Windows 2000 Server Dienst mutiert.

Ob Active Server Pages oder andere ISAPI-Anwendungen verwendet werden: nicht immer sind die IT-Abteilungen ebenso darüber erfreut, da sie den Einsatz des IIS gegenüber den permanenten Nachrichten über Hackerangriffe und Schwachstellen verteidigen müssen.

Doch hat Microsoft aus all den Fehlern gelernt, Security Patches und Tools stehen zur Verfügung. Allerdings haben viele IT-Abteilungen noch kein Know-How aufgebaut, das einen sicheren Betrieb von IIS gewährleistet. Und dies wird in der Zukunft immer wichtiger sein, da der IIS mittlerweile eine zentrale und obligatorische Rolle beim Exchange Server, bei SQLXML im SQL Server 2000 und in fast allen weiteren Backoffice Produkten spielt. Unter den .NET-Webservices ist der IIS fast überall dabei. Das heutige und zukünftige Web Storage System kommt ohne ihn nicht aus.

Das 3-tägige Seminar ".NET Internet Information Server" richtet sich an Entscheider, künftige IT-Administratoren des IIS, Adminstratoren von SQL-Server, Exchange und SharePoint Portal Server. Spezielle Vorkenntnisse sind zwar nicht erforderlich, aber Kenntnisse in Windows, Web und Datenbanken sowie TCP/IP-Grundlagen werden vorausgesetzt.

In diesem 3-tägigen Seminar mit praktischen Übungen am Rechner werden die unterschiedlichen Leistungsmerkmale, Features und Funktionen vorgestellt. Dabei werden viele Bestandteile live oder durch Videoaufnahmen demonstriert. Im Mittelpunkt stehen die Konfigurationswerkzeuge und Securitytools.

Das Seminar bietet die Möglichkeit, auch die realen Firmen-Szenarien der Seminarteilnehmer mit einzubeziehen und Vorschläge zu entwickeln. Als Versionen werden gleichermaßen der IIS 5.0 wie auch der IIS 6.0 unter .NET Server 2003 behandelt und praktisch demonstriert.

Der Trainer ist Hans Willi Kremer von der ComConsult Beratung und Planung

.NET ISA (Internet Security & Acceleration) Server

Daten müssen in einem immer größeren Umfang sowohl für interne als auch für externe Applikationen und Client-Systeme zugreifbar sein. Dies gilt Standort-intern, Standort-übergreifend aber auch für mobile Teilnehmer über das Medium Internet. Dabei soll die Übertragung der jeweiligen Daten schnell und kostengünstig erfolgen, steuerbar, kontrollierbar und gleichzeitig absolut sicher sein. All diesen Optionen wird der Microsoft Internet Security & Acceleration (ISA) Server 2000 gerecht.

Durch seine diversen Caching-Funktionen ist der Administrator in der Lage den gesamten ausgehenden und eingehenden Datenverkehr zu steuern und so z.B. den Bandbreitenverbrauch zu reduzieren. Daneben kann der ISA Server 2000 als Firewall konfiguriert werden, der mittels verschiedener Richtlinien die Sicherheit eines Unternehmensnetzwerkes erhöht, indem er den Datenverkehr überprüft und dann gegebenenfalls Pakete blockiert.

Das 2-tägige Seminar ".NET ISA Server" richtet sich an IT-Spezialisten, die die Schwerpunkte Netzwerksicherheit, Webadministration oder Netzwerkadministration haben und deren Unternehmen Produkte aus dem Microsoft Backoffice-Bereich einsetzen und befasst sich mit der Implementierung vom Microsoft Internet Security & Acceleration Server 2000.

Im Seminar demonstriert Hans Willi Kremer die zahlreichen Features, Funktionen und Merkmale des ISA Servers weitgehend live oder per Video. Themen des Seminars sind:

- Implementieren und Konfigurieren von ISA Server 2000 in Ihrem Netzwerk
- Einrichten eines Caching-Server
- Client-Konfigurationen
- ISA-Server als Firewall
- Zugriffssteuerung über Richtlinien und Regeln
- Überwachung der ISA-Aktivitäten
- Einsatz von ISA Server 2000 in einer AD-Domäne
- Migration von Proxy 2.0 nach ISA Server 2000

.NET SQL (Structured Query Language) Server

Auf dem Hintergrund von .NET werden Kenntnisse des SQL-Server immer wichtiger. SQL.Net weist den Weg zu einem universalen Data-Store für die künftigen Windows-Versionen.

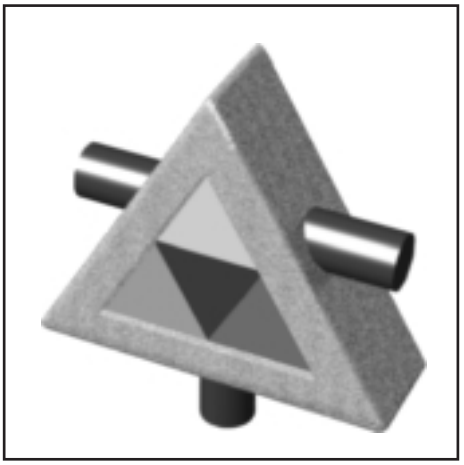
Das 3-tägige Seminar ".NET SQL Server" mit Praxisteil gibt einen Überblick über die Features, die SQL Server 2000 zur Verfügung stellt. Dabei wird auf die Schnittstellen zu Active Directory und den Office bzw. Backoffice-Produkten ebenso Wert gelegt wie auf die Erklärung der verschiedenen Datenzugriffspfade der Programmierwelt.

Ebenso sollen der künftig häufiger werdende Einsatz von Webservices mit SOAP und XML mit Datenzugriff auf den SQL-Server beleuchtet werden. Querverbindungen von SQL zu Office und Backoffice-Produkten und seine bisherige Integration in das Active Directory werden anschaulich dargestellt und diskutiert. In den Vorträgen werden die unterschiedlichen Leistungsmerkmale, Features und Funktionen vorgestellt. Dabei werden viele Bestandteile live oder durch Videoaufnahmen demonstriert.

Das Seminar richtet sich an Planer, Betreiber und Administratoren, die Microsoft Backoffice-Produktlinie im Unternehmensnetz einsetzen wollen. Spezielle Vorkenntnisse sind nicht erforderlich. Kenntnisse in Windows und Datenbankgrundlagen werden vorausgesetzt.

Der Referent Hans Willi Kremer ist bei der ComConsult Beratung und Planung GmbH als Berater im Kompetenz Center Backoffice tätig. Er besitzt langjährige Erfahrung insbesondere in seinen Spezialgebieten Exchange- und SQL-Server.

XML



Das Buch zum Seminar: "SELECT * FROM SQL Server 2000"

"Frisches Obst statt trockener Tabellen": SQL-Buch

Hans Willi Kremers Buch "SELECT * FROM SQL Server 2000" vom Galileo Verlag, knapp 1000 Seiten stark mit CD macht den Leser auf gut lesbare Weise durch verschiedene Zugangsmöglichkeiten mit Programmierung und Administration des SQL Servers vertraut.

Ein Quickstart-Teil führt in die Grundlagen ein. Danach werden alle wesentlichen Aspekte der serverseitigen Programmierung mit T-SQL vertieft, insbesondere Neuheiten wie benutzerdefinierte Funktionen, indizierte und partitionierte Views, deklarative Lösch- und Aktualisierungsweitergabe und Instead-Of-Trigger. Im administrativen Teil stehen Schnittstellen zu Windows 2000 Server, Sicherheit, Zugriffsrechte, Datenspeicherung, Backup und Replikation im Vordergrund. Der letzte Buchteil ist dem Thema SQL Server, Web und XML gewidmet. Das Buch umfasst damit den kompletten Umfang der SQL Server 2000-Zertifizierungsprüfungen. Der Leser findet verschiedene Elemente in diesem Buch vor: Durch Aufgaben kann er seine Kenntnisse vertiefen. Die Buch-CD enthält alle Codebeispiele und Lösungsvorschläge. Mehr als 150 Videoclips ermöglichen visuelles Lernen. Hyperlinks und Verweise eröffnen Ihnen den gezielten Zugang zu Informationen im Web und zu Artikeln der Onlinedokumentation. Tipps und Hilfe bei Zertifizierungsfragen zum MCDBA runden das Angebot des Buches ab.

Jeder Teilnehmer des ComConsult-Seminars ".NET SQL Server" erhält es kostenlos als Bestandteil der Seminarunterlagen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
.NET Seminare

.NET Server 2003 – plan

Ich melde mich für das Seminar (Einzelpreis: € 2.290,-- zzgl. MwSt.) zu dem angekreuzten Termin an:

☐ **10.03. - 14.03.03 Dorint Sporthotel Waldbrunnen in Windhagen-Rederscheid**

☐ **05.05. - 09.05.03 Hilton Bonn**

☐ **22.09. - 26.09.03 Courtyard by Marriott Düsseldorf Hafen**

NET Server 2003 – build & run

Ich melde mich für das Seminar (Einzelpreis: € 1.990,-- zzgl. MwSt.) zu dem angekreuzten Termin an:

☐ **24.03. - 27.03.03 Aachen AGIT, Dorint Quellenhof**

☐ **19.05. - 22.05.03 Linder Hotel BayArena in Leverkusen**

☐ **29.09. - 02.10.03 Park Plaza Köln**

Nutzen Sie unseren Paketpreis! Buchen Sie die Seminar-Reihe .NET Server 2003 – plan, build & run mit beiden Seminaren der Reihe und Sie zahlen (statt € 4.280,--) den vergünstigten Paketpreis von nur € 3.590,-- zzgl. MwSt.!

.NET Exchange Server

Ich melde mich für das Seminar zum Preis von € 1.990,-- zzgl. MwSt. zu dem angekreuzten Termin an:

☐ **24.03. - 27.03.03 Hilton Bonn**

☐ **03.06. - 06.06.03 Hilton Bonn**

☐ **10.11. - 13.11.03 Hilton Bonn**

.NET Internet Information Server

Ich melde mich für das Seminar zum Preis von € 1.590,-- zzgl. MwSt. zu dem angekreuzten Termin an:

☐ **10. - 12.03.03 Maritim Hotel Königswinter**

☐ **21. - 23.07.03 Hilton Bonn**

☐ **01. - 03.12.03 Hilton Bonn**

.NET ISA Server

☐ Ich melde mich für das Seminar vom **31.03. - 01.04.03** in der **BayArena Leverkusen** zum Preis von € 1.290,-- zzgl. MwSt. an.

.NET SQL Server

☐ Ich melde mich für das Seminar vom **17.03. - 19.03.03** im **Park Plaza Köln** zum Preis von € 1.590,-- zzgl. MwSt. an.

Ich melde mich für die oben angekreuzten Seminare an

☐ Buchen Sie für mich ein Zimmer im Hotel

Buchen Sie über unsere Web Site:
www.comconsult-akademie.de

Name, Vorname	Vorname
Firma	PLZ, Ort
Straße	eMail
Telefon, Fax	Unterschrift

Anzeige

Ausbildung zum ComConsult Certified Network Engineer

Nutzen Sie unsere Paketpreise!

3er Paket: Buchen Sie drei beliebige Seminare unserer Ausbildung zum ComConsult Certified Network Engineer und Sie zahlen statt € 5.970,-- nur den Paketpreis von € 5.190,-- zzgl. MwSt.

Komplett-Paket: Für die komplette Ausbildung mit allen vier Seminaren zum ComConsult Certified Network Engineer zahlen Sie statt € 7.960,-- nur den Paketpreis von € 6.690,-- zzgl. MwSt.

Das CCNE-Praxis-Seminar:

LAN-Praxis-Intensiv-Seminar:
Praktischer Aufbau von lokalen Netzen und Umsetzung typischer Netzwerk-Konfigurationen
Einzelpreis: € 2.290,-- zzgl. MwSt.
Zusätzlich zum Komplett-Paket: € 1.890,-- zzgl. MwSt.

- **05.05. - 09.05.03 in Aachen**

Termine 2003

Lokale Netze
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Aachen**
- **19.05. - 23.05.03 in Aachen**
- **21.07. - 25.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **10.11. - 14.11.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

TCP/IP und SNMP
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Berlin**
- **05.05. - 09.05.03 in Bonn**
- **21.07. - 25.07.03 in Berlin**
- **22.09. - 26.09.03 in Berlin**
- **13.10. - 17.10.03 in Berlin**
- **08.12. - 12.12.03 in Berlin**

Internetworking
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **10.03. - 14.03.03 in Aachen**
- **05.05. - 09.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

Neue Ethernet Technologien
Einzelpreis: € 1.990,-- zzgl. MwSt.

- **17.03. - 21.03.03 in Aachen**
- **12.05. - 16.05.03 in Aachen**
- **30.06. - 04.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**
- **13.10. - 17.10.03 in Aachen**
- **08.12. - 12.12.03 in Aachen**

ComConsult Akademie

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Optimale Netzstrukturen für hochverfügbare Serverfarmen, 24. - 26.02.03 in Köln

diskutiert die bestehenden Alternativen in der Anbindung von Servern und Speicher an Netzwerke. Denkbare Architekturen werden speziell unter dem Blickwinkel Performance, Verfügbarkeit und Betrieb gegenüber gestellt und bewertet.
Referent: Dr. Behrooz Moayeri (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

Integrierte Lösungen ... 24. - 26.02.03 in Bonn

Das Seminar beschäftigt sich mit der Voraussetzung für die Sicherstellung der Verfügbarkeit und der Performance der Unternehmenswichtigen Applikationen am Arbeitsplatz: eine funktionale und datentechnische Integration der einzelnen Management-Lösungen für Netzwerke, Server, Clienten und Applikationen.
Referenten: Dipl.-Verwaltungswirt Jürgen Dierlamm, Dr. Jürgen Suppan Preis: € 1.590,-- zzgl. MwSt.

OSPF und VRRP optimal konfigurieren, 25. -27.02.03 in Aachen

Das Seminar vermittelt die notwendigen Kenntnisse für die Migration und den erfolgreichen Betrieb von OSPF Netzen durch Live-Vorführungen unter Einsatz von Produkten führender Hersteller. Für ein umfassendes, Layer 3 basiertes Redundanzkonzept ist Router-Redundanz unverzichtbar. Optional kann am 4. Tag **1 Übungstag** (mit Übungstag € 1.990,-- zzgl. MwSt.) gebucht werden.
Referent: Markus Schaub (ComConsult Akademie) 3 Tage ohne Übungstag € 1.590,-- zzgl. MwSt.

IT-Projektmanagement II, 24. -28.02.03 in Aachen

Das Seminar ist der zweite von zwei Teilen der Ausbildung zum "ComConsult Zertifizierter IT-Projektleiter". Hier lernen die Teilnehmer Sitzungen zu moderieren, Projekte zu präsentieren, erfolgreich zu verhandeln und Projektteams zu leiten.
Referent: Dr. Ralf Hillemacher Einzelpreis: € 1.590,-- zzgl. MwSt.

Trouble Shooting in Lokalen Netzwerken - Grundlagen, 24. - 28.02.03 in Aachen

Das Seminar ist der erste von drei Teilen der Ausbildung zum "ComConsult Certified Trouble Shooter" und vermittelt das Fundament der erfolgreichen Fehlersuche in Lokalen Netzwerken.
Referenten: Dipl.-Inform. Oliver Flüs, Dr. Jochen Wetzlar Einzelpreis: € 2.490,-- zzgl. MwSt.

.NET IIS Server, 10. - 12.03.03 in Königswinter

Das Seminar baut Know-How auf, das einen sicheren Betrieb des Internet Information Servers gewährleistet, ohne den das heutige und zukünftige Web Storage System kommt nicht auskommt.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.290,-- zzgl. MwSt.

Cisco-Router erfolgreich einsetzen, 10. - 14.03.03 in Aachen

Das Seminar lehrt den Aufbau und die Arbeitsweise von Cisco-Routern an Cisco 2600 Routern, an denen die Teilnehmer aktiv arbeiten können. Referent: Markus Schaub Preis: € 2.590,-- zzgl. MwSt.

.NET Server 2003 – plan, 10. - 14.03.03 in Windhagen-Rederscheid

Das Seminar befasst sich mit der Strukturierung des Active Directory unter Windows .NET-Server 2003, wobei auch Mischszenarien mit Windows 2000 erläutert werden. Ein weiterer grundlegender Bestandteil ist das erforderliche IP-Management, insbesondere DNS.
Referenten: Markus Holländer, Dipl.-Inform. Michael van Laak, Frank Neunzig, Dipl.-Ing. Lars Kuhl Preis: € 2.290,-- zzgl. MwSt.

Internetworking, 10. - 14.03.03 in Aachen

Das Seminar vermittelt die technischen und methodischen Kenntnisse zur erfolgreichen Strukturierung von Netzwerken mit Switching und Routing wobei Grundlagen-Kenntnisse Lokaler Netzwerk-Technologien erforderlich sind.
Referentin: Dipl.-Inform. Petra Borowka Preis: € 1.990,-- zzgl. MwSt.

Ethernet in der Industrie, 10. - 14.03.03 in München

Das Seminar erklärt, wie ein Ethernet-Netzwerk in einer Produktions-Umgebung erfolgreich realisiert und betrieben werden kann.
Referenten: Dipl.-Ing. Peter Henkel, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Kai Lorentz Preis: € 1.990,-- zzgl. MwSt.

Sichere und flexible Vernetzung mit IP-VPNs, 12. - 14.03.03 in Berlin

Das Seminar beschäftigt sich mit den Vorteilen der flexiblen Möglichkeiten Internet-basierender VPNs und den erheblichen Risiken sowie den starken Abhängigkeiten von den anderen, bestehenden IT-Technologien, die die Realisierung eines VPN beinhaltet.
Referenten: Dipl.-Inform. Andreas Meder, Alexander Zarenko Preis: € 1.590,-- zzgl. MwSt.

Service Level Management in der Praxis, 17. - 19.03.03 in Köln

Das Seminar behandelt die Königsdisziplin des Netzwerk- und System-Managements: Service Level Management, wo die technischen und organisatorischen Fäden einer IT-Organisation zusammenlaufen und die zentrale Schnittstelle zwischen Betreibern und Anwendern innerhalb einer Firma oder zwischen externen Dienstleistern und Anwendern liegt.
Referenten: Heinz Hüsges und Martin Rother (Arxes NCC AG) Preis: € 1.590,-- zzgl. MwSt.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

.NET SQL Server, 17. - 19.03.03 in Köln

Das Seminar mit Praxisteil gibt einen Überblick über die Features, die SQL Server 2000 zur Verfügung stellt. Dabei wird auf die Schnittstellen zu Active Directory und den Office bzw. Backoffice-Produkten ebenso Wert gelegt wie auf die Erklärung der verschiedenen Datenzugriffspfade der Programmierwelt.
Referent: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

ITIL-Service Manager II, 17. - 20.03.03 in Bonn

Dieses Seminar der Ausbildung zum Zertifizierten Service Manager nach ITIL beschäftigt nach dem Foundation Exam und dem 2. Teil mit dem dem 2. Teil "Service Support" mit dem "Service Delivery', bevor die Ausbildung mit der Prüfung zum Certified ITIL Service Manager abgeschlossen werden kann.
Referenten: Thomas Engelmann und Dipl.-Kfm. Dipl.-Wirt. Inform. Bernd Holtz (Maxpert AG) Einzelpreis € 2.590,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 17. - 21.03.03 in Aachen

Das Intensiv-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: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan, ComConsult Akademie Preis: € 1.990,-- zzgl. MwSt.

TCP/IP und SNMP, 17. - 21.03.03 in Berlin

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referent: Matthias Hein Preis: € 1.990,--zzgl. MwSt.

Sicherheitslösungen für vernetzte IT-Umgebungen, 17. - 21.03.03 in Köln

Das Seminar beschäftigt sich mit modernen Sicherheitslösungen für den Internet-Zugang, das Mail-System, die Server, die Clienten und das Netz. Referenten: Das IT-Sicherheits-Team der ComConsult Beratung und Planung Preis: € 1.990,-- zzgl. MwSt.

Neue Ethernet-Technologien, 17. - 21.03.03 in Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dr. Joachim Wetzlar, ComConsult Beratung und Planung Preis: € 1.990,--zzgl. MwSt.

IT-Projektmanagement I, 17. - 21.03.03 in Bonn

Das Seminar ist der erste von zwei Teilen der Ausbildung zum "ComConsult Zertifizierter IT-Projektleiter". Hier lernen die Teilnehmer ein Projekt effektiv zu organisieren und überzeugend zu führen, sowie die Prozess-Optimierung der Projektabwicklung.
Referent: Dr. Ralf Hillemacher Einzelpreis: € 2.290,-- zzgl. MwSt.

Mobile und drahtlose Datenkommunikation..., 19. - 20.03.03 in München

Das Seminar gibt am 1. Tag einen Überblick über mobile und drahtlose Kommunikation, behandelt vertieft die GSM-Datendienste und zeigt die Möglichkeiten für die Unternehmenskommunikation auf und widmet sich am 2. Tag schwerpunktmäßig dem Wireless LAN.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Simon Hoff, Dr. Jochen Wetzlar Preis: € 1.290,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars

Vorname

Nachname

Termin

Firma

PLZ, Ort

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße

eMail

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Telefon, Fax

Unterschrift

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Netzwerk Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. 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

3Com Super Stack Dual Speed Hub 500 / 3C16611, Anzahl 3, Preis 240,00 Euro, Anzeigen-Nr. B21207

DEC 3 x Multi Switch 900, 3 x à 290,00 Euro, Power Supplies, 8 x à 50,00 Euro, VNswitch900EF, 1 x à 360,00 Euro, VNswitch900XX, 1 x à 300,00 Euro, DECswitch900EF, 4 x à 180,00 Euro, DECswitch900MX, 2 x à 360,00 Euro, Portswitch900CP, 2 x à 60,00 Euro, DECrepeater900TM, 1 x à 160,00 Euro, Anzeigen-Nr. B21208

3Com CoreBuilder 9000, Anzahl 1, Preis VS, 1 x 3CB9E16 CoreBuilder 9000 Chassis 2 x 3CB9LG9MC 9 x 1000Base-SX, SC 3 x 3CB9LF36R 36 x 10/100Base-TX, RJ45 2 x 3CB9FG24T Switch Fabric 48Gbps 1 x 3CB9LF10MC,10 x 100Base-FX, SC, 1 x 3CB9LG2MC, 2 x 1000Base-SX, SC, 2 x 3CB9EP8 Power Supply, 1 x 3CB9EMC Redundant Management Engine Controller, 1 x 3CB9EME Management Engine Anzeigen-Nr. B21216

Hub

DEC Hub 90, 3 x à 50,00 Euro, DECserver90L+, 2 x à 40,00 Euro, DECserver90M, 1 x à 40,00 Euro, DECrepeater90C, 7 x à 40,00 Euro, DECrepeater90FL, 2 x à 40,00 Euro, DECrepeater90T+, 1 x à 40,00 Euro, DECrepeater 90FA, 4 x à 40,00 Euro, DECbrouter90T1, 4 x à 120,00 Euro, DECbrouter90T2, 2 x à 120,00 Euro, Anzeigen-Nr. B21209

Gebote

Switch/Brücke

Madge Deskstream 24 Port Token Ring Switch, Anzahl >10, Preis 1.200,-- Euro VB, Bemerkung: Demo-Equipment, wie neu, incl. Garantie, incl. Stackingmodul, Ethernet und HSTR Uplinks ebenfalls vorhanden, Anzeigen-Nr. B21217

Cabletron
1 x MMAC-M8FNB à 200,00 Euro, 4 x M8PSM-E à 50,00 Euro, 5 x ESXMIM à 100,00 Euro, 1 x ESXMIM-F2 à 160,00 Euro, 1 x EMM-E6 à 180,00 Euro, Anzeigen-Nr. B21210

Cabletron
2 x ATX LANSwitch à 300,00 Euro, 2 x 3CPSM-R-ATX à 100,00 Euro, 6 x 3F00-01 à 120,00 Euro, 1 x 3H02-04 à 120,00 Euro, 1 x 3E08-04 à 80,00 Euro, 1 x 3E02-08 à 80,00 Euro, 1 x 3E02-04 à 40,00 Euro, Anzeigen-Nr. B21213

Enterasys
2 x SmartSwitch 9000/14-Slot à 700,00 Euro, 1 x SmartSwitch 9000/6-Slot à 400,00 Euro, 2 x 9C214-1 à 100,00 Euro, 2 x 9C206-1 à 50,00 Euro, 2 x 9F426-03 à 360,00 Euro, 1 x 9H421-12 à 720,00 Euro, 11 x 9H422-12 à 360,00 Euro, 2 x 9H423-28 à 390,00 Euro, 2 x 9E428-12 à 240,00 Euro, 8 x 9E423-36 à 360,00 Euro, Anzeigen-Nr. B21211

HP Pro Curve Switch 1600M / HP J4120A, Anzahl 1, Preis 480,00 Euro, Anzeigen-Nr. B21203

HP Pro Curve Switch 4000M / HP J4121A, Anzahl 1, Preis 1.280,00 Euro, Bemerkung: Inklusive: 5 x HP J4111A (8x10/100TP), 1 x HP J4118A (4x10FL), Anzeigen-Nr. B21204

HP Advanced Stack Switch 224T / HP J3177A, Anzahl 8, Preis 270,00 Euro, Anzeigen-Nr. B21202

Cisco Modell: 5002, Anzahl 1, Preis 260,00 Euro, Bemerkung: 1 x Chassis, 1 x Supervisor Engine, 1 x WS-X5213A, Anzeigen-Nr. B21201

3Com Super Stack II 300FX / 3C16982, Anzahl 1, Preis 660,00 Euro, Anzeigen-Nr. B21206

3Com Super Stack II Switch 3000 / 3C16981, Anzahl 1, Preis 360,00 Euro, Anzeigen-Nr. B21205

Cabletron Modell: ESX 1380, Anzahl 1, Preis 300,00 Euro, Bemerkung: Inklusive: 1 x BRIM-E100, 1 x FE100-FX, Anzeigen-Nr. B21214

Gebote

Switch/Brücke

Enterasys
1 x 2E42-27R à 240,00 Euro, 2 x HSIM-F6 à 120,00 Euro, 6 x FE100-TX à 30,00 Euro, 3 x FE100-FX à 60,00 Euro, Anzeigen-Nr. B21215

Fax an ComConsult 02408/955-399

☐ **Ich suche**

☐ **Ich biete**

☐ **Antwort auf Anzeigen-Nr.** ☐ _____

Produkt/Komponente/Release/Software

_____

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon

_____

Fax

_____

eMail

Weitere Anzeigen

finden Sie auf dem Web-Server der ComConsult Akademie

www.comconsult-akademie.de