

Dokumentation zur betrieblichen Projektarbeit

Aktualisieren einer Firewall



Fachinformatikerin Fachrichtung Systemintegration
Abschlussprüfung Sommer 2001

Vorgelegt von
Wiebke Schneider

Wiebke Schneider
Azubi-Ident: 161/743565
Prüflings-Nr: 161/51018
Abschlussprüfung Sommer 2001
01197 Fachinformatikerin Systemintegration

Persönliche Erklärung:

Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbstständig erstellt habe.

Ort und Datum

Unterschrift der Auszubildenden

Inhaltsverzeichnis

1	Ausgangssituation.....	1
1.1	Die Firma	1
1.2	Themen-Ursprung.....	1
1.3	Zielbestimmung	1
2	Zeitlich gegliederter Projektablauf	1
3	Ist-Analyse.....	2
3.1	Das Netzwerk	2
3.2	Eingesetzte Hardware	2
3.3	Eingesetzte Software.....	2
4	Soll-Konzept	4
4.1	Anforderungen an die Firewall.....	4
4.2	Risikoanalyse.....	6
4.3	Bestimmung der Möglichkeiten	6
4.4	Die Alternativen	7
4.5	Kosten-Analyse.....	9
4.6	Auswertung.....	9
5	Durchführung	10
5.1	Das Testsystem	10
5.2	Einarbeitung.....	11
5.3	Aktualisierte Filterregeln	12
5.4	Regeln implementieren und testen.....	13
5.5	Integration in das Netzwerk – Inbetriebnahme	13
6	Qualitätssicherung	13
6.1	Abschließender Funktionstest	13
6.2	Notwendige Anpassungen?.....	14
6.3	Sicherung für Notfälle	14
7	Projektabschluss	15
7.1	Projektkosten	15
7.2	Rückschau	15
7.3	Ausblick.....	16
7.4	Dokumentation.....	16
8	Quellennachweis.....	16
9	Anhang.....	17
	Netzwerkplan I	A
	Netzwerkplan II	B
	Das Testsystem	C
	Konfiguration des Firewall-Rechners	D
	Leistungsumfang der betrachteten Firewalls	E
	Angebote	F
	Detaillierte Preisübersicht	G
	Investitionsantrag	H
	Firmendokumentation	I
	Nessus Scan Report	J
	Glossar	K

1 Ausgangssituation

Das vorliegende Projekt fand in dem Zeitraum vom 1. 03. 2001 bis zum 1. 04. 2001 hausintern bei der Firma Hüppe GmbH & Co. OHG statt.

1.1 Die Firma

Die Firma Hüppe in Bad Zwischenahn stellt Duschabtrennungen der gehobenen Klasse her und vertreibt diese über die jeweiligen Standorte in ganz Europa. Am Hauptstandort Bad Zwischenahn sind ca. 250 Mitarbeiter beschäftigt, davon verwenden etwa 200 das EDV-System für ihre Arbeit.

Die Firma gehört zu dem amerikanischen Konzern Masco, mit dem auch ein regelmäßiger Datenabgleich stattfindet.

1.2 Themen-Ursprung

Aufmerksam geworden durch die Bemerkung eines Mitarbeiters, der behauptete, sein Bekannter könne jederzeit in das firmeninterne Netzwerk einbrechen, sowie durch die allgemein zunehmenden Hacker-Attacken auf Firmennetzwerke (z. B. Microsoft) wurde eine Überprüfung der Netzwerksicherheit geplant. Durch die gesteigerte Aufmerksamkeit wurde tatsächlich ein verdächtiger Zustand bemerkt, der nun die Aktualisierung oder Neu-Konzipierung der Firewall erforderlich macht.

1.3 Zielbestimmung

Die zurzeit eingesetzte Firewall soll auf Sicherheitslücken geprüft und entweder mit einer neueren Version upgedatet, oder aber durch ein anderes dem aktuellen Stand der Technik entsprechendes Produkt ersetzt werden. Beide Vorgehensweisen sind denkbar und müssen daher mit ihren jeweiligen Vor- und Nachteilen betrachtet werden.

Das Projekt umfasst die Einholung von entsprechenden Angeboten, das Abwägen beider Varianten sowie die anschließende Planung und Umsetzung der gewählten Lösung.

2 Zeitlich gegliederter Projektablauf

Projektphase	Inhalte	Arbeitsaufwand (h)		Datum der Durchführung
		geplant	real	
Zielbestimmung	Informationsgespräch/Projektantrag	(1,0)	(1,0)	13. 02. 01
Projektplanung	Projektablaufplan	2,0	1,5	02. 03. 01
Ist-Analyse	Netzwerk	1,5	1,5	05. 03. 01
	Hardware/Software	1,0	1,0	05. 03. 01
	Filterregeln	1,5	2,0	05. 03. 01
Soll-Analyse	Anforderungsanalyse	1,5	1,5	08. 03. 01
	Angebote einholen	2,0	3,0	09. 03. 01 – 14. 03. 01
	Alternativen bestimmen	1,0	1,0	15. 03. 01
	Kosten-Analyse	2,0	3,0	15. 03. 01
	Entscheidungsgespräch	1,5	1,5	16. 03. 01
	Präzisierte Zielbestimmung	1,0	0,5	16. 03. 01
Durchführung	Beschaffung Hard/Software	1,0	1,0	19. 03. 01 – 23. 03. 01
	Einarbeitung	3,0	2,0	26. 03. 01
	Testsystem aufbauen	1,5	1,5	26. 03. 01
	Installation	1,5	0,5	26. 03. 01
	Konfiguration	4,0	2,5	27. 03. 01
	System testen	2,0	2,0	27. 03. 01
	Inbetriebnahme	3,0	1,5	28. 03. 01
Qualitätssicherung	Funktionstest	1,5	1,5	28. 03. 01
	Sicherung anlegen	0,5	0,5	28. 03. 01
Projektabschluss	Dokumentation	1,0	3,0	29. 03. 01
	Übergabe	1,0	2,5	30. 03. 01
Gesamt		35,0	35,0	

3 Ist-Analyse

3.1 Das Netzwerk

Die europäischen Standorte der Firma sind mit dem Hauptstandort in Bad Zwischenahn über Wähl- oder Standleitungen verbunden. Überwiegend handelt es sich dabei um IBM Global Network-Verbindungen. Der Standort in den Niederlanden wird über eine ISDN-Leitung mit Hilfe eines Bintec-Routers angebunden.

Das lokale Netzwerk ist eine Token-Ring-Topologie mit insgesamt fünf Ringen, die über einen zentralen Switch miteinander verbunden sind. Internet und Intranet trennt eine Linux-Firewall und ein kleines Netzwerk auf Ethernet-Basis. In diesem Screened Subnet sind BNC-Kabel verlegt, wohin gegen der Token-Ring mit verdrehten Kabeln der Kategorie 5 ausgestattet ist.

An das Netzwerk¹ sind ca. 250 NT-Workstations angeschlossen. Die Serverfarm besteht aus 18 NT-Servern, zwei Linux-Servern und einer AS/400. Sie fungieren als Anmelde-, File-, Print-, Internet-, Datenbank-, Mail-, DNS-, und DHCP-Server. Einen Webserver betreibt das Unternehmen zurzeit noch nicht vor Ort. Dessen Einrichtung vor Ort ist jedoch angedacht und soll bei der Realisierung der Firewall-Lösung berücksichtigt werden. Ebenfalls zu bedenken sind eine zukünftige Erweiterung der 64 KBit/s ISDN-Anbindung ins Internet auf eine 2 MBit/s Standleitung und der Einsatz von VPN.

3.2 Eingesetzte Hardware

Die zurzeit eingesetzte Firewall besteht aus drei Bintec-Routern und einem Compaq Deskpro EP Series Rechner mit zwei Netzwerkkarten.

Angaben zu Ausstattung und Funktionsumfang der Geräte finden sich als Legende auf dem Netzwerkplan im Anhang.

Alle vier Geräte sind den zurzeit an sie gestellten Datendurchsatz-Anforderungen voll gewachsen. Aus dieser Sicht sind also bei Bestehenbleiben der aktuellen Lösung keine weiteren Überlegungen anzustellen.

3.3 Eingesetzte Software

Firmennetzwerk:

Eine Firewall filtert unter anderem nach Protokollen, Portnummern und IP-Adressen. Daher müssen die in der Firewall zu konfigurierenden Ports ermittelt werden. Hierzu wurden alle relevanten eingesetzten Anwendungen (hausintern, Außendienstmitarbeiter und Niederlassungen) dokumentiert und die benutzten Ports ermittelt².

Anwendungen	Protokolle	Ports	Verwendung
Lotus Notes 5.0	TCP	1352	Mails der Außendienstmitarbeiter
VIS 2000	NetBIOS	137-139	Datenbank für Außendienstmitarbeiter
IBM Client Access	TCP	23 und andere	AS/400 Zugriff von außen
Rumba NT	TCP	23	AS/400 Zugriff von außen
Citrix	TCP		Externer Citrix-Server
Internet-Explorer 5.0	HTTP	Über Port 3128	Webzugriff für das LAN und die Niederlande
Netscape 4.5	HTTP	Über Port 3128	Webzugriff für das LAN
NetSupport	TCP		Remote-Administration
Sendmail	SMTP	25	Mailtransfer
Telnet	TCP/UDP	23	Wartungsarbeiten
Auth	TCP/UDP	540	Authentisierung
Ident	TCP/UDP		Authentisierung
Ping	ICMP	0	Analyse
News	NNTP	119	Administrationswerkzeug
FTP	FTP	21,20	Administration, Datentransfer intern

¹ Ein Netzwerkplan findet sich im Anhang A.

² <http://www.belwue.de/wwwservices/hilfestellungen/ulm/faq/port-num.htm>
Kurtz: Das Anti-Hacker-Buch S. 529ff.

Die Tabelle zeigt Anwendungen und Protokolle, die in unterschiedlicher Form über das Internet betrieben werden. Sie müssen daher bei der Konfiguration einer Firewall berücksichtigt werden.

Die Firma setzt einige Anwendungen ein, auf die von Außendienstmitarbeitern zugegriffen wird. Besonders diese Anwendungen müssen bei der Konfiguration der Firewall berücksichtigt werden.

Betriebssystem und Konfigurations-Software:

Die Router sind die Schnittstellen des firmeninternen Netzwerkes zur Außenwelt. Bintec1 stellt eine ISDN-Verbindung für die Internetkommunikation der Mitarbeiter bereit. Bintec2 wird mit vier Telefonnummern zur Einwahl von außen genutzt. Die holländische Niederlassung wird per Telefonleitung über einen weiteren Router (Bintec3) angebunden.

Die drei Router verfügen über eigene, sehr einfach gehaltene Paketfilter. Da diese für die Betrachtung der zu aktualisierenden Firewall jedoch keine Rolle spielen, wird in dieser Projektarbeit nicht auf das implementierte Regelwerk eingegangen.

Bei der bisher verwendeten Firewall handelt es sich um ein SuSE-Linux der Version 6.2 mit einem Kernel in der Version 2.2.10. Die Firewall wurde von einer externen Firma installiert und in gemeinsamer Arbeit konfiguriert. Alle Updates und sonstigen Wartungen der Firewall gehen von Mitarbeitern der Firma Hüppe aus und werden selbst ausgeführt oder explizit in Auftrag gegeben.

Als Firewall ist ein reiner Paketfilter in Kombination mit dem in der Distribution enthaltenen Web-Proxy-Dienst installiert. Aus Sicherheitsgründen kann hier keine genaue Wiedergabe der implementierten Paketfilterregeln erfolgen. Einen Eindruck davon können jedoch die im Anhang D zusammengefassten Filterregeln vermitteln. Diese dienen im Verlauf des Projektes auch als Vorlage für die aktualisierten Firewall-Regeln.

Neben dem Firewall-Dienst bietet der Rechner auch noch weitere Dienste im Netzwerk an: Bind (DNS), Sendmail (Mail), Squid (HTTP-Proxy), Routing, Telnet und Samba.

Im HTTP-Proxy Squid sind zur Kontrolle des Internetzugriffs einige Zugriffsbeschränkungen hinterlegt. Zur Definition von Zugriffsgruppen werden extra angelegte Text-Dateien aufgerufen. Diese enthalten zum Beispiel verbotene URLs und bestimmte Textteile der URLs, Gruppen von IP-Adressen oder einige Dateierweiterungen, die zum Download gesperrt sind.

Die Datei „/var/log/messages“, in der Linux-Systeme Log-Meldungen ablegen, ist in diesem Fall gelöscht. Dafür sind mehrere einzelne Log-Dateien angelegt. In diese werden die Meldungen vom System sortiert eingetragen.

Diese Konfiguration hat zwei Vorteile:

- Die Meldungen werden sortiert abgelegt und können daher mit weniger Zeitaufwand genutzt werden.
- Ein Einbrecher kann seine Spuren nicht durch das Standardvorgehen, nämlich Löschen der Datei „messages“, verbergen.

Es wurden für die Administratoren eigene Benutzerkonten mit Root-Rechten eingerichtet.

Der Root-Account wurde deaktiviert, indem sein Shell-Eintrag in der rc.config auf „false“ gesetzt wurde. Daher muss ein Angreifer neben dem Passwort auch einen Benutzernamen ermitteln, um Root-Rechte zu erlangen.

Es ist ein Support-Benutzer (externe Firma) mit sehr einfach zu erratenden Passwort eingerichtet.

Der Benutzer „nobody“, der auch vom System für einige Vorgänge verwendet wird, hat keine direkte Anmeldemöglichkeit, da ihm kein Passwort zugeordnet ist. Daher funktioniert das Gastlogin nicht.

Zur Datensicherung über das Netzwerk und dem Dateizugriff von einem Windows-Rechner aus, ist der Samba-Dienst so konfiguriert, dass Passwörter verschlüsselt übertragen werden. Folgende Freigaben sind eingerichtet:

Homes	Mailtransfer	Sicherung
comment = Heimatverzeichnis browseable = no read only = no create mode = 0750	comment = User mail-transfer ressource path = /usr/mail-transfer read only = no locking = no	comment = Sicherung path = / read only = no locking = no public = yes browseable = yes read list = aaa, bbb, ccc write list = aaa, bbb, ccc directory mask = 0770

Zusammenfassung

Das gesamte Softwaresystem eines Firewall-Rechners wirkt sich auf die Sicherheit dieser Firewall aus. Übersehene Sicherheitslücken des Betriebssystems oder einzelner Teile der installierten Software könnten von Hackern zum Angriff auf das System ausgenutzt werden.

Während der Durchführung der Ist-Analyse sind einige Einstellungen der Firewall aufgefallen, die Risikofaktoren darstellen, und unter Umständen den Einbruch ermöglichen. Diese wurden soweit möglich sofort beseitigt, und sollen hier kurz dargestellt werden.

Grundsätzlich gilt: fehlerfreie Programme gibt es nicht. Genauso wenig wie 100 %ige Sicherheit. Je weniger Software installiert ist, desto kleiner ist das Risiko. Firewall-Systeme sollten daher besonders schlanke Systeme sein.

Das betrachtete Firewallsystem bei Hüppe enthält neben den genutzten Programmteilen auch eine Anzahl an überflüssigen Anwendungen³. Soweit möglich sollten diese Softwareteile deinstalliert werden.

Die Firewall führt, wie aus dem letzten Abschnitt ersichtlich, neben dem Firewall-Dienst noch etliche andere Dienste aus. Bei einigen Diensten (Sendmail, Bind, Samba) handelt es sich um etwas ältere Versionen, in denen bekannte Sicherheitslücken bestehen. Diese sollten unbedingt durch aktuelle Versionen ersetzt werden.

Im Samba sind speziellere Sicherheitsrisiken aufgefallen (siehe oben).

Samba ist als recht risikoreich einzuschätzen, da es seine Aufgabe ist, Daten im Netzwerk bereitzustellen. Es muss also sehr genau darauf geachtet werden, welche Daten freigegeben werden, und wer Zugriff darauf hat. Bei genauer Betrachtung haben sich in der vorliegenden Samba-Konfiguration folgende Schwachstellen aufgetan: Mit der Freigabe „Sicherheit“ wurde den angegebenen Benutzern der Zugang zum Wurzelverzeichnis gewährt!

Außerdem ermöglichte die Einstellung „public=yes“ jedem beliebigen, dem System nicht bekannten User (wird dann als „nobody“ eingestuft) ebenfalls mit Gast-Rechten den Zugriff auf die Root. Dem User „nobody“ war kein Passwort zugeordnet, daher ist eine Anmeldung zunächst nicht möglich, allerdings war irgendein, vielleicht einmal probenhalber vergebenes Passwort für diesen Benutzer ausreichend, damit jeder fremde Benutzer völlig ohne Passwort auf die Freigabe zugreifen können!

Die Einstellung „browseable=yes“ macht die Freigabe zudem in der Netzwerkumgebung sichtbar!

Zur Beseitigung dieses Sicherheitsrisikos wurde die Einstellung „public=yes“ herausgenommen. Die Freigabe des Wurzelverzeichnisses ist zurzeit für die zentral über das Netzwerk gesteuerte Datensicherung mit ARCserveIT notwendig und blieb daher bestehen. Das gleiche gilt für die Sichtbarkeit im Netzwerk.

4 Soll-Konzept

Es geht dem Unternehmen darum, eine aktuelle, dem momentanen Stand der Technik entsprechende Firewall einzusetzen. Dadurch soll, unter Beachtung wirtschaftlicher Gesichtspunkte, ein für dieses Unternehmen optimaler Schutz des Firmennetzes erreicht werden.

Das bedeutet: Viel Sicherheit durch ein aktuelles Produkt zu einem vertretbaren Preis.

Um ein geeignetes Produkt zu bestimmen, ist es notwendig eine detaillierte Analyse der Anforderungen an die Firewall durchzuführen.

4.1 Anforderungen an die Firewall

Eine Firewall beinhaltet einen Paketfilter und eventuell einen Application Level Gateway. Es können viele verschiedene Einstellungen vorgenommen werden. Diese verwendet die Firewall zur Filterung aller IP-Pakete. Je nach passender Regel werden die Pakete entweder weitergeleitet, zurückgewiesen oder verworfen.

Je nach Arbeitsweise und Beschaffenheit des lokalen Netzwerkes hat jede Firma ihre eigenen Ansprüche an den Internetzugang. Bei Hüppe haben sich nach Betrachtung der Infrastruktur folgende Notwendigkeiten ergeben:

- Es muss möglich sein, anhand der **IP-Adressen** (Quelle und Ziel eines IP-Paketes) über dessen Weiterleitung zu entscheiden. Auf diese Weise können Berechtigungen (z. B. zum FTP-Download aus dem Internet) an bestimmte IP-Adressen gebunden werden, um so für einige Mitarbeiter den Download zu ermöglichen, für die übrigen jedoch nicht.
- Ebenso muss nach **Portnummern** unterschieden werden, damit zum Beispiel Außendienstmitarbeiter ihre E-Mails vom internen Notes-Server abholen können, ohne dass für sie gleich der gesamte Zugang geöffnet werden muss.

³ Siehe Anhang D

- Es handelt sich hier um ein Netzwerk mit privaten IP-Adressen. Da diese von einem Router nicht in das Internet weitergeleitet werden und somit die Datenpakete/Internetanfragen aus dem Intranet keine gültigen Quell-IP-Adressen haben, muss die Firewall über eine Masquerading-Funktion verfügen. Hiermit wird die Übersetzung der privaten IP-Adressen in offizielle und umgekehrt vorgenommen (**NAT=Network Address Translation**).
- Das Herunterladen von Dateien aus dem Internet bedeutet ein zusätzliches Viren-Risiko und belastet in nicht zu unterschätzendem Maße die Verfügbarkeit des Internetzuganges. Daher ist es wichtig eine **Downloadbeschränkung** bestimmen zu können.
- Die Downloadbeschränkung sollte sich nicht nur auf das Herunterladen von Dateien beziehen, sondern darüber hinaus das Filtern von Webseiten-Inhalten (**Content Filter**) anhand ausgewählter Stichwörter und URLs erlauben. Diese Funktion kann zum Beispiel durch einen externen **Smart Filter** (Siemens-Produkt) erreicht werden. Solche Filter beinhalten eine Art Ausschluss-Liste mit bestimmten URLs. Sie werden von einigen Firmen zentral gepflegt und kommerziell angeboten.
- Verschiedene **Proxies**: HTTP, SMTP und wenn möglich FTP.
- Proxies bieten differenziertere Filtereinstellungen als reine Paketfilter, was sich allerdings bei der Verarbeitungsgeschwindigkeit bemerkbar machen kann. Diese Filtereinstellungen ermöglichen es Webseiten nach bestimmten Kriterien zu beurteilen, sodass zum Beispiel sexuelle Inhalte nicht abgerufen werden können. Mit einem SMTP-Proxy können E-Mail-Header von unnötigen Informationen, die einem Angreifer nützlich sein könnten (z.B. IP-Adressen und Computernamen der Mailserver oder das verwendete Mail-Programm), befreit werden.
- Da Hüppe wiederholt Ärger mit extrem umfangreichen E-Mails (bis zu 110 MB) hat, wäre es vorteilhaft, wenn E-Mails in Abhängigkeit von ihrer **Größe** gefiltert werden könnten, bevor sie überhaupt in das lokale Netzwerk gelangen.
- Geschwindigkeit (Throughput = **Datendurchsatz**) ist durch die ständig zunehmenden Anforderungen an den Internetzugang ein wichtiges Kriterium. Zurzeit gehen Daten aus 6 ISDN-Leitungen⁴ durch diese Firewall. Das heißt, der maximale Durchsatz beträgt im Moment $4 \times 64 \text{ Kb/s} = 384 \text{ Kb/s}$. Da in naher Zukunft allerdings eine Anbindung mit 2 Mb/s geplant ist, sollte die Firewall mindestens 3 Mb/s verarbeiten können.
- **Aktive Inhalte** auf Webseiten enthalten Programmstrukturen. Diese Strukturen können sich zerstörerisch auf den empfangenden PC (Software und Daten) auswirken. Die gängigen Browser verfügen daher über eine Funktion zur Ablehnung solcher Webseiten mit aktiven Inhalten. Diese Funktion muss allerdings an jedem Rechner einzeln aktiviert werden. Das Herausfiltern an einem zentralen Punkt (normalerweise im HTTP-Proxy) spart Zeit und Mühe. Außerdem wird eine nicht autorisierte Beeinflussung dieser Einstellung am Browser umgangen.
- Da der Mail-Server im LAN durch die Firewall geschützt werden muss, dieser jedoch für den Mail-Server des Provider erreichbar sein muss, ist es notwendig, dass die Firewall über die Möglichkeit des **Portforwarding** (Port-Weiterleitung) verfügt.
- Die Firewall sollte über ein **VPN-Modul** verfügen, da die Firma plant die Außendienstmitarbeiter und auch die ausländischen Niederlassungen demnächst über das Internet anzubinden, um so Telefonkosten einzusparen.
- Die **Passwörter** für Außendienstmitarbeiter sollten hinterlegt werden können. Schön wäre die Authentifizierung mit Hilfe der NT-Benutzerverwaltung.
- Die Konfiguration sollte so übersichtlich wie möglich gehalten sein. Dazu gehört auch eine gut und überschaubar strukturierte **Konfigurationssoftware**, die bei einem derartig komplexen Thema zur Vermeidung von Konfigurationsfehlern beiträgt.
- Die Konfigurationen müssen extern gesichert werden können, um so im Fehlerfall eine schnelle Wiederherstellung zu ermöglichen (**Policy-Sicherung**).
- Da auf Grund der Weiterentwicklung des Unternehmens immer wieder neue Anforderungen hinzukommen werden, ist auf die **Anpassungsfähigkeit** und Erweiterbarkeit der Firewall zu achten.
- Die **Fernadministrierbarkeit** ist vor allem dann von Bedeutung, wenn die Wartung vollständig oder teilweise an externe Firmen vergeben wird, oder aber das notwendige Know-how in der Firma bei wenigen Mitarbeitern liegt, was hier der Fall sein wird. Die Fernwartung sollte aus Sicherheitsgründen mit Hilfe von **verschlüsselten Zugriffsverfahren** wie zum Beispiel SSL erfolgen.
- Für den Fall, dass einmal ein Angriff stattgefunden hat, ist es besonders wichtig, diesen zu bemerken. Auf **Angriffserkennung** und die Qualität der verschiedenen **Log-Files** ist daher ebenfalls zu achten.
- Die Firewall sollte **IP-Spoofing** (Fälschung der Quell-IP) erkennen und abwehren. Mit IP-Spoofing kann ein Angreifer seine eigene IP-Adresse (über die er zu identifizieren wäre) verschleiern. Zudem wird ein System Antworten auf Pakete von gespooften IP-Adressen an den falschen Absender verschicken und kann so zur Ausführung von DDoS-Attacken auf andere Systeme missbraucht werden.

⁴ ISDN-Leitungen: 1x Internetanbindung (Bintec1), 4x Einwahl via ISDN, 1x Hollandverbindung via ISDN

Für die Sicherheit einer Firewall ist neben dem Produkt vor allem der zuständige Administrator verantwortlich.⁵ Die Firma Hüppe möchte die Administration ihrer Firewall betriebsintern durchführen, da auf diese Weise das Know-how bei den Mitarbeitern der Firma entwickelt wird. Dadurch wird unter anderem die Umsetzung von Konfigurationsänderungen vereinfacht und beschleunigt, was Kosteneinsparungen bedeuten kann.

Da die Verwaltung der Firewall möglichst von einem Firmenmitarbeiter durchgeführt werden soll, ist bei der Auswahl des Produktes auf die Übersichtlichkeit der Management-Software in besonderem Maße Wert zu legen.

4.2 Risikoanalyse

Ein Unternehmen, das einen Internetzugang nutzt, sollte sich des Einbruchs-Risikos und daraus möglicherweise resultierender Schäden bewusst sein⁶.

Entgegen der häufigen Meinung, von Hackerangriffen seien nur große Firmen wie Microsoft betroffen, sind auch alle anderen Internetanschlüsse gefährdet. Kleinere und mittelständische Unternehmen sind das Ziel von unerfahrenen Angreifern, die auf diesem Gebiet ihre Erfahrungen sammeln. Hier werden ungeplante, mutwillige Angriffe auf mehr oder weniger zufällige Ziele ausgeführt. Unerfahrene Angreifer sind dabei nicht minder gefährlich als erfahrene, denn sind sie erst einmal in das Netzwerk gelangt, richten sie dort absichtlich oder unabsichtlich häufig großen Schaden an⁷. Der Datenbestand eines Unternehmens ist sein Kapital. Wenn dieser Datenbestand beschädigt, entwendet oder manipuliert wird, kommen schnell enorme Schadenssummen zustande.

Um kritischen Daten handelt es sich zum Beispiel bei den Konstruktionszeichnungen und Design-Entwürfen, die bei Hüppe angefertigt werden. Ein Verlust der Zeichnungen wäre schlimm und der Schaden kaum kalkulierbar. Die unbemerkte Manipulation würde unter Umständen dazu führen, dass eine ganze Produktionsreihe nicht mehr zu gebrauchen wäre. Auch besteht das Risiko einer Entwendung der Daten (Industriespionage) durch ein Konkurrenzunternehmen. Der Fall, dass Daten der nächsten Kollektion vorzeitig bekannt werden, muss, wenn irgendwie möglich, ausgeschlossen werden.

Wird die Firewall beschädigt, muss der Internetzugang bis zur Wiederherstellung geschlossen werden. In dieser Zeit ist das Unternehmen nicht mehr per E-Mail zu erreichen, und die holländische Niederlassung kann nicht mehr auf die AS/400 zugreifen, was einem vollständigen Arbeitsausfall an diesem Standort gleichkommt.

Gelingt es einem Einbrecher die AS/400 lahm zu legen, steht auch an alle anderen Standorten der Vertrieb. Die Daten werden zwar täglich vollständig auf DLT-Kassetten gesichert, dennoch vergehen einige Stunden, bis die AS/400 wieder einsatzbereit ist.

Auch eine Firewall garantiert keinen 100 %igen Schutz vor Angriffen aus dem Internet, aber sie stellt eine Möglichkeit da, das Risiko zu minimieren. Sicherheitsbestimmungen gehören bei der Firma Hüppe fest zum Unternehmenskonzept. Die Firewall ist *ein* Teil davon.

4.3 Bestimmung der Möglichkeiten

Variante 1

Das jetzige Linuxsystem wird aktualisiert.

Grundsätzlich wären wiederum zwei Vorgehensweise denkbar:

- a) Update auf eine neuere Version
- b) Neuinstallation einer aktuellen Version mit Übertragung der jetzigen Konfiguration

Ein Update von SuSE 6.x auf SuSE 7.x ist nach Aussagen einiger Kollegen nicht unproblematisch. Zudem bekommt man durch eine Neuinstallation ein reines System, von dem eine Sicherung angelegt werden wird, so dass es im Zweifelsfalle schnell wieder in den Grundzustand zu versetzen ist, wenn es zu einer Veränderung durch Eindringlinge gekommen sein sollte. Auch werden eventuelle diesbezügliche Altlasten auf diese Weise ausgeschlossen.

Hier wird als Variante 1 also die Neuinstallation mit Übertragung/Prüfung und Anpassung der zurzeit verwendeten Konfigurationen betrachtet. Ziel ist es, ein möglichst kompaktes, sicheres und zügig wiederherstellbares System zu schaffen.

⁵ Strobel: Firewalls S. 7

⁶ Auf eine detaillierte Darstellung der jeweiligen Schadenssummen wird hier verzichtet, da die Ermittlung den Rahmen des Projektes sprengen würde.

⁷ <http://www.alldas.de/>

Variante 2

Ein ganz anderes Produkt kommt zum Einsatz.

Im Rahmen dieses Projektes ist es nicht möglich, alle auf dem Markt befindlichen Firewall-Lösungen zu betrachten, daher muss schon zu diesem Zeitpunkt eine Auswahl getroffen werden. Die Auswahl gründet sich auf bestehende Angebote einiger Firmen, sowie auf die bereits seit einigen Jahren bestehenden Geschäftsbeziehungen mit anderen Firmen. Hinzu kommen zwei (GeNUGate und Securepoint) Produkte deutscher Hersteller, die eine Recherche im Internet ergab.

Im Einzelnen sollen hier vier Produkte berücksichtigt werden:

- a) Checkpoint Firewall-1
- b) WatchGuard Firebox II
- c) GeNUGate
- d) Securepoint Firewall Server

4.4 Die Alternativen

Der Leistungsumfang der einzelnen Produkte ist in einer Übersicht im Anhang E beigefügt.

SuSE 7.1

Der Linux-Distributor SuSE bringt etwa im Abstand von je einem halben Jahr eine neue Version seines SuSE-Linux auf den Markt. Aktuell ist dies die Version 7.1. Erstmals beinhaltet diese Version den Kernel 2.4 und das neue Firewall-Programm Netfilter (iptables). Netfilter ist in seiner Funktionalität sehr vielversprechend⁸ (zum Beispiel stateful filtering), allerdings zeigen sich bei neuen Programmen in der ersten Einsatzzeit erfahrungsgemäß diverse Sicherheitslücken. Daher sollte man bei einem so kritischen Einsatzbereich, wie es die Firewall eines Unternehmens ist, die Beseitigung dieser Kinderkrankheiten abwarten. SuSE 7.1 kann auch mit dem bewährten Kernel 2.2 installiert werden und mit ipchains arbeiten. Da auch das bisherige System ipchains verwendet, könnte das Regelwerk so problemlos übertragen werden.

Das SuSE 7.1 ist ein vollständiges Betriebssystem, das sowohl als Workstation wie auch als Server arbeiten kann. Zusätzlich sind eine Reihe von Anwendungsprogrammen enthalten. SuSE 7.1 wird auf 10 CDs ausgeliefert, was einen ungefähren Eindruck von der mitgelieferten Softwaremenge vermittelt.

Als ursprüngliches Server-Betriebssystem hat es einen großen Funktionsumfang, der allerdings für eine Firewall-Installation größtenteils unnötig ist⁹.

Wie viele andere Distributoren von Linux-Systemen, versucht auch SuSE bereits seit einigen Jahren ein möglichst benutzerfreundliches Arbeitssystem zu schaffen, das auch der „normale“ Heimanwender einsetzen kann. Viele Einstellungen können daher inzwischen über grafische Tools vorgenommen werden. Leider gibt es für das Firewall-Programm ipchains nach wie vor kein überzeugendes grafisches Konfigurationstool.

Checkpoint Firewall-1

Die Firewall-1 ist eine Software-Firewall der amerikanischen Firma Checkpoint. Sie ist eine der verbreitetsten Firewall-Lösungen überhaupt. Häufig wird sie im Bundle mit einem extra für diesen Zweck abgesicherten Betriebssystem und entsprechender Hardware angeboten.

Es liegt ein solches Bundle-Angebot der Firma Vistorm vor. Dabei handelt es sich um eine Hardwarebox mit Nokia-Betriebssystem, Firewall-1-Software und einer optional zu integrierenden VPN-Lösung.

Vistorm ist ein britischer Anbieter mit Standort in Düsseldorf. Sie bieten die Installation, Konfiguration und Wartung der Firewall an. Abhängig vom Preis kann das auch ein 24 h Rundumservice sein.

Die Checkpoint hat einen enormen Leistungsumfang, der unseren Anforderungen (siehe Abschnitt 4.1) voll gerecht wird¹⁰.

Besonders hervorzuheben ist die große Anzahl vordefinierter Filterregeln und die eigene Benutzerverwaltung (auch Gruppen). Bezogen auf diese Gruppen können Filterregeln erstellt werden. Es können URLs oder auch Web-Inhalte herausgefiltert werden. Dazu stellt Checkpoint eine sehr umfangreiche vordefinierte Auswahl bereit (Content Filter).

⁸ <http://netfilter.samba.org/unreliable-guides/netfilter-hacking-HOWTO/index.html>

<http://www.linuxia.de/lt-netfilter.en.html>

⁹ siehe Abschnitt 3.3

¹⁰ Die ausführliche Beschreibung des Leistungsumfanges findet sich bei <http://www.checkpoint.com>

Durch den Stateful Inspection-Filter werden Datenpakete auf ihren Inhalt untersucht, sodass die Firewall manipulierte Datenpakete sicherer identifizieren kann.

Kommen an unterschiedlichen Unternehmensstandorten mehrere Checkpoint-Firewalls zum Einsatz, so können diese zentral administriert werden.

WatchGuard Firebox II

Die Firma WatchGuard bietet die Firebox in vier Varianten an: Firebox Soho, Firebox II, Firebox II Plus, Firebox II Fast VPN. Die Firebox Soho ist auf Grund ihrer begrenzten Leistungsfähigkeit ausschließlich für kleine Büros gedacht und kommt daher für Hüppe nicht in Frage. Variante zwei und drei unterscheiden sich lediglich durch ihre Hardwareausstattung und die daraus resultierende Belastbarkeit. Die Firebox II Fast VPN ist für den verstärkten Einsatz von VPN gedacht und verfügt zur verschlüsselten Datenübertragung daher über ein extra VPN-Steckmodul. Für Hüppe ist nach meiner Einschätzung und den Aussagen der anbietenden Firmen die Firebox II vollkommen ausreichend.

Die Firebox II ist eine kombinierte Hard- und Software-Firewall. Das heißt, es handelt sich um ein Gerät (19"-Technik) mit 3 Ethernet Netzwerkinterfaces und für den Firewallbetrieb optimiertem Betriebssystem. Im Falle der Firebox II ist die Plattform ein Linuxsystem mit Kernel 2.0.33.

Zur Konfiguration wird eine umfangreiche und übersichtliche Management-Software ausgeliefert¹¹.

Für die Firebox II wurden Angebote von drei in Deutschland ansässigen Firmen (Messerknecht-Meister, Bents, Sunday) eingeholt, da die US-amerikanische Firma WatchGuard das Produkt in Deutschland nur über Distributoren vertreibt.

Die Firebox II unterstützt neben der eigenen auch die Benutzerverwaltung mit Hilfe von Radius, SecureID, CryptoCard oder NT. Sie kann mit einem NT-Server zusammenarbeiten, das heißt, dessen Benutzerdatenbank nutzen. Da bei Hüppe NT-Server zur Benutzerverwaltung eingesetzt werden, könnte eine einheitliche, zentrale Administration der Benutzerkonten erreicht werden.

Besonders interessant ist auch das dazugehörige LiveSecuritySystem: Die Software-Updates, die regelmäßig aufgrund des LiveSecuritySystems vollautomatisch, geliefert werden, werden mit RSA-Verschlüsselung übertragen. Die Echtheit der Software wird mit dem MD5 Hash-Algorithmus sichergestellt.

GeNUGate

Die GeNUGate ist ein Produkt der Firma GeNUA in München. Es handelt sich um eine kombinierte Soft- und Hardware-Lösung in drei verschiedenen Ausstattungsstufen.

Die GeNUGate beinhaltet neben einem Paketfilter auch den Application Level Gateway. Als Plattform verwendet die Firewall ein angepasstes BSD-System (eine Unix-Variante).

Sowohl der Application Level Gateway, als auch der Paketfilter können per Web-Browser konfiguriert werden.

Hardwareseitig besteht die GeNUGate aus zwei kompletten Rechnersystemen mit jeweils eigener CPU, die zusammen in einem Gehäuse untergebracht sind. Der Application Level Gateway verfügt über eine eigene Festplatte, sodass auch ein Caching von Webseiten mit einem Proxy eingerichtet werden kann. Neben dem HTTP-Proxy sind weitere transparente Proxydienste (SMTP, FTP, Gopher, WAIS, TCP für PPTP, UDP, Telnet, NNTP, POP3) konfigurierbar.

Securepoint Firewall Server

Der Securepoint Firewall Server ist eine Linux basierende Firewall. Sie kann als reine Software-Lösung (ein Firewall-System für einen Standard-PC) erworben werden, im Bundle mit einem Pentium im 19"-Gehäuse oder auch vorinstalliert auf einem standard Compaq Deskpro.

Mit Hilfe einer einfachen Management-Software ist die Securepoint Firewall über das LAN von einem bestimmten Windows oder Linux-PC konfigurierbar. Dabei erfolgt die Datenübertragung mit ssh verschlüsselt. Das Betriebssystem Linux wurde auf die Aufgaben einer Firewall zugeschnitten. Das heißt, es werden nur Pakete installiert, die für diese Funktion notwendig sind.

Die Software kann unter <http://www.securepoint.de> heruntergeladen und 30 Tage getestet werden.

Mit einem Preis von 1750 DM für die Software ist die Securepoint eine vergleichsweise kostengünstige Firewall-Lösung.

¹¹ Informationen zur Firebox II finden sich auf der Website des Herstellers (<http://www.watchguard.com>).

4.5 Kosten-Analyse

In der folgenden Tabelle sind alle fünf Alternativen in einer Preisübersicht dargestellt. Detaillierte Angaben zur Zusammensetzung und Begründung der einzelnen Angaben sind im Anhang G aufgeschlüsselt.

	SuSE 7.1	WatchGuard	Checkpoint	Securepoint	GeNUGate
Produkt	2.129,00 DM	9.999,00 DM	87.092,00 DM	4.199,00 DM	22.609,39 DM
Garantie und Support für 1 Jahr		2.189,00 DM	10.228,00 DM		9.025,18 DM
Schulung ¹²	6.190,00 DM				
Einrichtung	1.200,00 DM	800,00 DM	35.400,00 DM	400,00 DM	4.561,00 DM
Hausinterner Wartungsaufwand für 12 Monate	5.200,00 DM	2.400,00 DM	2.400,00 DM	2.400,00 DM	2.400,00 DM
Gesamt für das erste Jahr	14.719,00 DM	13.199,00 DM	135.120,00 DM	6.999,00 DM	38.595,57 DM
Kosten für ein weiteres Jahr	5.200,00 DM	4.589,00 DM	12.628,00 DM	2.400,00 DM	11.425,18 DM
Kosten für die ersten 3 Jahre	25.119,00 DM	22.377,00 DM	160.376,00 DM	11.799,00 DM	61.445,93 DM
Bemerkungen	keine Garantieleistung	Der Support für das erste Jahr ist im Produktpreis enthalten.	Einrichtung durch Vertragspartner; Wartung hausintern	keine Garantieleistung; Schulung nicht notwendig	Einrichtung durch Vertragspartner; Wartung hausintern

Es wird deutlich, wie stark die Firewall-Lösungen sich im finanziellen Bereich unterscheiden. Die Securepoint ist innerhalb der betrachteten Auswahl die weitaus günstigste Firewall-Lösung. Allerdings ist sie mit ihrem Leistungsumfang an der untersten Grenze. Aufgrund des fast vollständig fehlenden Supports und der recht dünnen Einstellungsmöglichkeiten, kommt der Securepoint Firewall Server für die Firma Hüppe nicht in Frage.

4.6 Auswertung

„Sicherheit“ kostet Geld! Mit einer Sicherheitslösung können nur bedingt konkrete Kosteneinsparungen erreicht werden. Diese sind vornehmlich durch Reduzierung des Administrations- und Wartungsaufwandes erreichbar.

Standard-Linux-Systeme sind in der Anschaffung sehr günstig, allerdings benötigt der Administrator vergleichsweise viel Know-how, um damit umgehen zu können. Das bedeutet, regelmäßige Schulungen und Praxiserfahrung sind notwendig. Wartung und Pflege eines solchen Firewall-Systems sind aufwendig und zeitintensiv. Fehler und Hintertüren in Open Source Software wie Linux werden von einer großen Gemeinde untersucht und, zusammen mit entsprechenden Bugfixes öffentlich dokumentiert. Das gewährleistet auf der einen Seite, dass einem engagierten Administrator kaum eine Lücke in seinem System verborgen bleibt, gleiches gilt allerdings auch für die Angreifer. Daher ist es dringend zu empfehlen, sich beim Einsatz eines solchen Systems um bekannt werdende Schwachstellen zu kümmern. Das kostet täglich viel Zeit. In unserem Fall müsste sich bei der Entscheidung für das SuSE Linux 7.1 ein Mitarbeiter täglich mit der Firewall beschäftigen. Beim Fixen von irgendwelchen Schwachstellen garantiert niemand die Echtheit und Vertrauenswürdigkeit des Patches und auch nicht, dass es das eigene Firewallsystem nicht in irgendeiner Weise beschädigt.

Auch die Securepoint ist eine auf Linux basierende Firewall. Patches werden vom Hersteller auf dessen Website zur Verfügung gestellt. Allerdings ist die Securepoint Firewall noch ein recht unbekanntes System, sodass einerseits nicht so viele Schwachstellen bekannt sind, andererseits aber auch existierende Schwachstellen beim Administrator möglicherweise unbemerkt bleiben. Im Gegensatz zu dem SuSE Linux ist es ein schlankes Firewall-Betriebssystem, dass auf Sicherheit ausgelegt ist. Außerhalb der Möglichkeiten, die das Windows-Konfigurationstool bietet, können auf einem Securepoint Server kaum Einstellungen vorgenommen werden. Das Tool hat jedoch recht begrenzte Einstellungsmöglichkeiten.

¹² Die Administration eines Linux-Systemes erfordert die umfangreiche Kenntnis des Betriebssystems. Diese können in einer Schulung erworben werden.

Im krassen Gegensatz dazu stehen die ebenfalls auf Linux basierende Firebox II und GeNUGate (BSDI). Beide Systeme bieten umfangreiche Einstellungsmöglichkeiten und ein gut organisiertes Update-System. Wobei die GeNUGate-Lösung hardwaretechnisch sehr aufwendig gemacht ist, bei der Firebox dagegen vor allem Wert auf den Support gelegt wurde. Bei vergleichbaren Funktionen ist die GeNUGate jedoch etwas teurer als die WatchGuard¹³.

Als das einzige Nicht-Linux-System in dieser Vergleichsreihe fällt die Checkpoint Firewall-1 besonders durch ihren enorm hohen Anschaffungspreis auf. Der Vertreiber Vistorm, von dem das im Anhang F befindliche Angebot stammt, betonte zwar mehrfach, dieses seien nur Richtpreise über die verhandelt werden kann, allerdings sticht die Checkpoint im Preisvergleich sehr weit aus den übrigen Lösungen heraus. Beim CeBIT-Besuch am Checkpoint-Stand fiel vor allem der modulartige und sehr komplexe Aufbau der Firewall-1 auf. Es handelt sich sicherlich um ein sehr leistungsfähiges Produkt, dass allerdings beim Preisvergleich extrem aus dem Rahmen fällt, und daher gegenüber der Unternehmensleitung kaum zu vertreten wäre.

Die fünf beschriebenen Firewall-Lösungen wurden der Abteilungsleitung in einem Gespräch vorgestellt. Aus den folgenden Überlegungen haben wir uns für die WatchGuard Firebox II entschieden:

- Sie zeigt aus unserer Sicht ein gutes Preis-Leistungs-Verhältnis.
- Sie wird den gestellten Anforderungen gerecht.
- Die Firebox verfügt über eine, für dieses komplexe Thema, besonders einfach zu bedienende Konfigurationssoftware.
- Da die Wartung der Firewall im eigenen Haus stattfinden soll, ist besonders die fast vollständig automatisch organisierte Updatefunktion mit der LiveSecurity sinnvoll.
- Es war kein Problem, ein Testgerät zu bekommen, um sich mit der Firebox II vertraut zu machen.
- WatchGuard ist ein relativ großer, auf Security spezialisierter Hersteller, der seine Produkte weltweit vertreibt. Daher ist die Infrastruktur recht umfangreich. Bei auftretenden Fragestellungen gibt es eine Reihe von fachkundigen Anlaufstellen und Online-Hilfen.
- Die Firebox ist ein ausgereiftes Produkt, dass bereits seit mehreren Jahren auf dem Markt ist. Sie ist inzwischen bei Version 4.6 angelangt und wird auch weiterhin verbessert und ausgebaut.

Für den Kauf der WatchGuard Firebox II kommen drei im Umland ansässige Vertragspartner in Frage: Messerknecht-Meister, Sunday und Bents Informationssysteme.

Von allen drei Firmen wurden Angebote¹⁴ eingeholt. Wir haben uns für die Firma Bents entschieden, da sie uns das günstigste aller Angebote machen und auch umgehend und kostenfrei ein Testgerät zur Verfügung stellen konnte, mit dem die dieser Projektarbeit zugrundeliegende Konfiguration durchgeführt wurde.

Nach diesem Gespräch wurde ein entsprechender Investitionsantrag¹⁵ bei der Geschäftsführung gestellt. Die Genehmigung steht zum Zeitpunkt der Erstellung dieser Dokumentation allerdings noch aus.

5 Durchführung

5.1 Das Testsystem

Es wurde zunächst einmal ein Testsystem aufgebaut. Auf diesem Wege sollte die Funktionsweise erprobt und die Gestaltung der Regeln erarbeitet werden. Die verwendete Hardware war bis auf die Firebox II in der Firma verfügbar und musste daher nicht extra beschafft werden.

Bestandteile des Testsystems:

ISDN-Router:	Elsa Lancom Office 1000
Firewall:	Firebox II
Ethernet-Hub:	D-Link 10/100 Mbit/s
Management-Station:	Windows NT Workstation 4.0 WatchGuard LiveSecurity-Software zwei Netzwerkkarten (Ethernet, Token-Ring)

¹³ siehe Übersicht im Anhang E und G

¹⁴ siehe Anhang F

¹⁵ siehe Anhang H

Das Testsystem¹⁶

Die WatchGuard Firebox II hat drei Netzwerk-Schnittstellen: Eine zum *external Network*, eine zum *trusted Network* und eine weitere für ein *optional Network*, die sogenannte DMZ (demilitarisierte Zone).

Über das *external Network* wird die Verbindung mit dem Internet hergestellt. Hierzu wurde diese Schnittstelle mit dem ISDN-Router verbunden.

Am *trusted Interface* wurde ein kleines Ethernet mit der WatchGuard und der Management-Station eingerichtet. Die Management-Station stellte später auch die Verbindung zum Token-Ring basierten Firmennetzwerk her.

Das *optional Interface* blieb im Testsystem ungenutzt.

Die Management-Station

Die Firebox II verfügt nicht über eigenen Monitor, Tastatur oder Maus. Zur Einrichtung, Konfiguration und Wartung des Gerätes wird daher ein zweiter Rechner (minimal: Pentium, 64 MB RAM, 40 MB HDD, CD-ROM, Windows 9x oder NT ab SP4) benötigt.

Im Lieferumfang der Firebox II ist eine spezielle Konfigurationssoftware enthalten. Diese wird zunächst auf einem PC installiert, um so auf die Firewall zugreifen zu können.

Die Firma Hüppe setzt in ihrem Netzwerk fast ausschließlich Windows NT 4.0 Workstation als Arbeitsplatzrechner ein. Da der für die Zeit des Praktikums zur Verfügung gestellte PC ein solcher Arbeitsplatzrechner (entspricht den obigen Anforderungen) ist, wurde auf eine separate Installation auf einem extra Rechner verzichtet und dieser Arbeitsplatzrechner als Management-Station verwendet. Dadurch entfällt der Aufwand für eine Windows NT-Installation. Die Installation der Managementsoftware ist eine Standardsoftwareinstallation, auf die einzelnen Installationsschritte soll daher an dieser Stelle nicht ausführlich eingegangen werden. Anfängergerechte Hilfestellung bietet darüber hinaus der mitgelieferte InstallGuide. Zusätzlich zur eigentlichen Software werden bei der Installation umfangreiche Dokumentationen in Adobes Acrobat-Format bereitgestellt.

Nach erfolgter Installation wird der Rechner neu gebootet, woraufhin der Setup-Wizard¹⁷ für die erste Erstellung einer grundlegenden Policy startet. In einer Reihe unterschiedlicher Dialogfenster werden die notwendigen Angaben eingetragen. Die Dialogfenster sind übersichtlich gestaltet und eine passende Hilfefunktion steht jederzeit im HTML-Format zur Verfügung.

Der Setup-Wizard stellt schließlich über das Netzwerk die erste Verbindung mit der Firebox her und überträgt dabei die soeben erstellte Konfiguration.

Die Konfiguration der Firebox II:

Die Firebox kann in zwei unterschiedlichen Modi arbeiten. Sie kann an allen drei Interfaces die gleiche IP-Adresse nutzen (Drop-in-Mode) oder im „Routed Mode“ drei verschiedene IP-Adressen verwenden. Da die Firebox später zwei unterschiedliche logische Netzwerke miteinander verbinden soll, wurde das Testsystem im Routed Mode installiert. Dabei wurden die folgenden Adressen zugewiesen:

ISDN-Router:	172.17.1.254
Firebox - external:	172.17.1.1
Firebox - optional:	172.18.1.1
Firebox - internal:	172.19.1.1
Management-Station:	172.19.1.85

Als Subnetmask wurde jeweils die 255.255.0.0 eingestellt. Im Test wurden Klasse B IP-Adressen verwendet, damit die Konfiguration später mit möglichst wenig Aufwand für den Einsatz im Firmennetzwerk angepasst werden kann.

5.2 Einarbeitung

Zum Lieferumfang der WatchGuard gehört ein InstallGuide und der UserGuide. Darüber hinaus sind noch einige PDF-Dateien als Online-Hilfe verfügbar. Auf der Webseite von WatchGuard kann ein Trainingskurs absolviert werden. Alle Texte sind in englischer Sprache verfasst und inhaltlich recht einfach gehalten, sodass auch ein unerfahrener Benutzer damit zurechtkommt. Allerdings gehen dadurch meiner Ansicht nach wichtige Inhalte verloren, die notwendig sind, wenn keine einfache Standardfirewall umgesetzt werden soll. Diese musste ich mir daher durch Probieren erarbeiten.

In einigen Bereichen waren Rückfragen an den Distributor Wick Hill notwendig.

Um die Arbeitsweise der Software kennen zu lernen, wurden zunächst einige einfache Test-Policies umgesetzt.

¹⁶ Foto im Anhang C

¹⁷ siehe Firmendokumentation im Anhang I

5.3 Aktualisierte Filterregeln

Durch den Systemwechsel von Linux zur Firebox II müssen die Regeln neu angelegt werden.

Es wurde eine Überprüfung des ursprünglichen Regelkataloges¹⁸ vorgenommen. Wie bereits angemerkt, ließ dieser allerdings in einigen Bereichen mehr Zugriffe zu, als erforderlich sind. Da dieses ein zusätzliches Risiko darstellt, wurde das neue Regelwerk entsprechend enger gefasst.

Konkret ergibt sich für die Firma das folgende Regelwerk:

Wert	Richtung	Protokoll	Anwendung	Port	Quell-IP/Benutzer	Ziel-IP
Accept	ankommend/ausgehend	TCP/UDP	Programmierer	Jeder	Programmierer	AS/400
Accept	ankommend/ausgehend	TCP	Wartung	23	Ext. Firma	RS/6000
Accept	ankommend/ausgehend	TCP	Wartung	ftp	Ext. Firma	RS/6000
Accept	ankommend/ausgehend	TCP	Datenbankzugriff	1494	PC1	Citrix-Server
Accept	ankommend/ausgehend	TCP	Datenbankzugriff	1494	PC2	Citrix-Server
Accept	ankommend/ausgehend	TCP	Datenbankzugriff	1494	PC3	Citrix-Server
Accept	ankommend/ausgehend	TCP	Datenbankzugriff	1494	PC4	Citrix-Server
Accept	ausgehend	TCP	News	119	Gruppe Admins	Jede
Accept	ausgehend	TCP	MSN-Messenger	1080	PC5	Jede
Accept	ankommend/ausgehend	TCP	Mail-Transfer	25	Provider-Mail-Server	Mail-Relay1
Accept	ankommend	TCP	Mail-Transfer	25	Mail-Relay2	Mail-Server
Accept	ankommend	TCP	Wartung	Auth	Mail-Relay2	Mail-Server
Accept	ankommend	TCP/UDP	Wartung	Ident	Mail-Relay2	Mail-Server
Accept	ankommend/ausgehend	TCP	Wartung	NetBIOS	File-Server	Mail-Server
Accept	ankommend/ausgehend	TCP	Mail-Transfer	1352	Notes-Server	ADM
Accept	ankommend/ausgehend	TCP	Wartung	23	RS/6000	Ext. Firma
Accept	ankommend/ausgehend	TCP	HüppeNL	23	HüppeNL	AS/400
Accept	ankommend/ausgehend	TCP/UDP	HüppeNL	1352	HüppeNL	Notes-Server
Accept	ankommend/ausgehend	TCP/UDP	Wartung	5405	AdminPC	HüppeNL
Accept	ankommend/ausgehend	TCP/UDP	Router-Verb.	540	Router NL	AdminPC1
Accept	ankommend/ausgehend	TCP/UDP	Router-Verb.	540	Router NL	AdminPC2
Accept	ankommend/ausgehend	TCP	Router-Konf.	23	AdminPC	Bintec1
Accept	ankommend/ausgehend	TCP	Router-Konf.	23	AdminPC	Bintec2
Accept	ankommend/ausgehend	TCP	Router-Konf.	23	AdminPC	Bintec3
Accept	ankommend/ausgehend	TCP/UDP	Mail-Relay-Konf.	ftp	AdminPC6	Mail-Relay2
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	23	AdminPC6	Mail-Relay2
Accept	ankommend/ausgehend	TCP/UDP	Mail-Relay-Konf.	NetBIOS	AdminPC6	Mail-Relay2
Accept	ausgehend	ICMP	Ping		LAN	Jede
Accept	ankommend/ausgehend	TCP/UDP	Datenübertragung	NetBIOS	File-Server	Mail-Relay2
Accept	ankommend	UDP	Syslog-UDP	540	Bintec1	Protokoll-Rechner
Accept	ankommend/ausgehend	TCP	DNS-Datenbank-Abgleich	53	Mail-Relay2	Mail-Relay1
Accept	ausgehend	TCP	Pflege der E-Mail-Adressen beim Provider	8383	Gruppe Admins	Provider
DENY	ankommend/ausgehend	alles	alles	Jeder	Jede	Jede

¹⁸ siehe Abschnitt D im Anhang

5.4 Regeln implementieren und testen

Die neuen Regeln wurde mit Hilfe der LiveSecurity-Software (Policy Manager)¹⁹ im Testsystem eingerichtet. Als Grundlage hierzu diente das neu erstellte Regelwerk²⁰. Die Einstellungen wurden soweit möglich im Testsystem geprüft. Auf Grund der Komplexität des Netzwerkes war es jedoch nicht möglich, alle notwendigen Regeln zu testen. So konnte zum Beispiel der von extern kommende Zugang auf die AS/400 im Testnetzwerk nicht überprüft werden. Dies betrifft auch den FTP-Zugang, den eine externe Firma für Wartungsarbeiten im Netzwerk nutzt, den Zugriff auf einen externen Citrix-Server von einigen Arbeitsstationen im Netzwerk und den Mailtransfer mit dem Provider. Entsprechende Tests wurden daher erst im Produktivnetzwerk durchgeführt²¹.

5.5 Integration in das Netzwerk – Inbetriebnahme

Da der Internetzugang der Firma ein wichtiger Bestandteil des täglichen Arbeitslebens in der Firma Hüppe ist, muss gewährleistet sein, dass dieser nicht über einen längeren Zeitraum behindert wird. Zur Integration der Firebox in das Produktivnetzwerk waren daher einige Vorbereitungen notwendig.

Die Firebox sollte wie im Netzwerkplan II ersichtlich²² in das vorhandene Netz eingefügt werden. Sie übernimmt dabei die IP-Adresse des bisherigen Firewall-Rechners. Die Firebox kann den Firewall-Rechner nicht ersetzen, da dieser außer der Firewall-Funktion noch einige andere Dienste (Sendmail, DNS, Proxy, ...) im Netzwerk bereit stellt. Zudem verfügt die WatchGuard über drei Ethernet-Interfaces, sodass eine Übersetzung von Ethernet zu Token-Ring (LAN) stattfinden muss. Die Firebox nimmt stellvertretend für den SMTP-Dienst des alten Firewall-Rechners die E-Mails vom Provider entgegen und reicht sie mit Hilfe des Portforwarding an diesen weiter. Das bedeutet, dass es notwendig ist, einige Einstellungen des Firewall-Rechners zu verändern, damit dieser trotz der Veränderungen im Netzwerk weiterhin seine Dienste ausführen kann. Zu diesem Zweck wurden von allen zu verändernden Konfigurationsdateien zwei Versionen angelegt, die dann bei der Integration in das Netzwerk bzw. Herausnahme hin und her kopiert werden konnten. Auf diese Weise ist ein sehr schneller Wechsel zwischen einem Netzwerk mit Firebox und einem ohne sie möglich.

Für die Clients war das Wechseln vollständig transparent, denn der Gateway für die Arbeitsstationen im Netzwerk blieb weiterhin der alte Firewall-Rechner.

Änderungen mussten an den DNS-Zonen-Dateien, den Einträgen im „mailertable“ (Sendmail), der „rc.config“ (IP-Adresse der Netzwerkkarte und Masquerading) und in der eigentliche Firewall-Datei „/sbin/init.d/firewall“ (ipchains) vorgenommen werden. Nach dem Wechsel muss ein Neustart durchgeführt werden.

Das Wechseln funktionierte problemlos. Ein Umschalten war innerhalb von weniger als 5 Minuten möglich.

Die Protokollierung der Firebox wurde für jeden Filter aktiviert, damit eine Auswertung des Log-Files Aufschluss über das Greifen oder nicht Greifen der Regeln geben konnte.

Vor der Integration in das Produktivnetzwerk wurden einige Mitarbeiter über das Vorhaben informiert und gebeten ihre Zugriffe während der Testphase zu überprüfen.

6 Qualitätssicherung

6.1 Abschließender Funktionstest

Wie in der Darstellung der Filterregeln in Abschnitt 5.3 deutlich wird, muss die Firewall von Hüppe viele verschiedene Zugriffe ermöglichen. Da die neue Firewall eine Veränderung in der Struktur des Netzwerkes mit sich bringt, und die neuen Regeln um einiges enger gestaltet wurden (es soll nur möglich sein, was unbedingt notwendig ist), muss das Funktionieren der einzelnen Zugriffe beim Einsatz des Gerätes überprüft werden.

Im Einzelnen mussten folgende Zugriffe getestet werden:

- Anfragen an den DNS-Dienst (Web)
- Telnet-Anfragen (Wartung durch eine externe Firma, Rumba der niederländischen Niederlassung, Programmierer)
- E-Mail-Transport (Sendmail)
- Proxy-Dienst (Squid -> Web)
- Routing Durchgänge (z. B. bei der Einwahl eines Außendienstmitarbeiters)
- AS/400-Drucken aus den Niederlanden
- IP-abhängige Regeln testen (Citrix, Samba auf dem Mail-Relay, Mail-Adressen-Wartung, ...)

¹⁹ Erläuterungen zur Handhabung und Screenshots finden sich in der Firmendokumentation im Anhang I

²⁰ siehe Abschnitt 5.3

²¹ siehe Abschnitt 6.1

²² siehe Anhang B

- Administration (Zugriff von der Management-Workstation auf die Firebox)
- Reaktion auf Angriffe -> Logfiles -> Warnmeldungssystem (getestet mit nessus ²³)

Anmerkung: Als Ergebnis eines Angriffes mit einem der bekanntesten Security-Scanner bekam ich unzählige Warnmeldungen des Warnmeldungssystems der Firebox per E-Mail, mit der Meldung, es habe einen Portscan gegeben.

Der Scanner konnte außer einer wilden Spekulation über das hinter der angegriffenen IP-Adresse stehende Betriebssystem keine Informationen nennen. Das ansonsten sehr gute Tool behauptet, es handele sich bei der Firebox um ein „multivoip“-System. Das ist ein Modul, das bei Voice over IP zum Einsatz kommt ²⁴. Ein Vergleichsscan auf eine eigene Linux-Firewall (mit Standard-Einstellungen) ergab ein wesentlich ausführlicheres Ergebnis ²⁵.

6.2 Notwendige Anpassungen?

Als wir die Firebox in das Firmennetzwerk integrierten, waren noch einige Anpassungen notwendig.

- Welche Ports von der in den Niederlanden zum AS/400-Drucken eingesetzten Software verwendet werden, konnte erst während des abschließenden Funktionstests ermittelt werden. Der Filter wurde entsprechend angepasst.
- Die IP-Adresse des Citrix-Servers bei dem Mutterkonzern Masco stimmte nicht mehr mit der zur Zeit der Einrichtung dieses Zuganges dokumentierten Adresse überein. Bisher führte dies nicht zu Behinderungen, da das Script der Linux-Firewall jeglichen Zugang zu Citrix-Servern ermöglichte.

Den Angaben nach Rücksprache mit den zuvor informierten Mitarbeitern zufolge, haben schließlich alle Zugänge auch mit der neu erstellten Firewall-Lösung funktioniert.

6.3 Sicherung für Notfälle

Die WatchGuard hält das Betriebssystem und die Einstellungen in einem Flash-ROM. Sie verfügt nicht über Festplattenspeicher. Dieser Flash-Speicher ist in zwei Bereiche aufgeteilt: In dem einen Bereich wird die aktuell verwendete Software gespeichert, in dem anderen Bereich kann ein Backup-Image abgelegt werden. Zusätzlich wird jede Konfigurations-Datei immer auch auf der Management-Station gespeichert. Da die Konfigurationsdateien üblicherweise nur einige Kilobyte umfassen, kann die Sicherung zusätzlich auch auf einer Diskette erfolgen.

Zur Wiederherstellung einer früheren Konfiguration bietet die WatchGuard mehrere Möglichkeiten:

- Die Wiederherstellung des Backup-Images mit Hilfe eines Assistenten ist eine Möglichkeit. Dieses Verfahren kann verwendet werden, wenn vorläufig erstellte Veränderungen wieder rückgängig gemacht werden sollen. Voraussetzung hierfür ist allerdings, dass das Image vor den Veränderungen erstellt wurde.
- Eine weitere Möglichkeit ist das Einspielen einer externen, z.B. auf einer Diskette, gesicherten Konfigurationsdatei. Zu diesem Zweck wird eine Kopie der Konfigurationsdatei auf eine Diskette gespeichert und diese an einem sicheren Ort verwahrt.
- Zur Wiederherstellung wird der Policy-Manager an der Management-Station geöffnet, die Konfigurationsdatei von der Diskette geöffnet und in die Firebox gespeichert. Hierbei sollte auch gleich ein neues Image auf der WatchGuard erzeugt werden.
- Auch falls es nicht mehr möglich sein sollte, sich mit der WatchGuard zu verbinden, ist die ursprüngliche Konfiguration vergleichsweise schnell wiederherzustellen. Dies setzt allerdings voraus, dass eine aktuelle und funktionstüchtige Kopie der Policy-Datei existiert.
- Hierzu wird die WatchGuard in ihren Auslieferungszustand zurückgesetzt und anschließend mit dem Setup-Wizard eine neue Grundkonfiguration erzeugt. Diese kann dann durch die gesicherte Policy-Datei ersetzt werden.
 - WatchGuard ausschalten.
 - Zwei der drei Netzwerk-Schnittstellen mit einem gekreuzten Kabel verbinden.
 - Die Management-Station mit einem Netzwerk-Kabel (gekreuzt oder mit Hub) oder auch mit dem beiliegenden seriellen Kabel mit der WatchGuard verbinden.
 - Auf der Management-Station den Setup-Wizard starten. Den Anweisungen des Assistenten folgen ²⁶. Nachdem alle notwendigen Angaben zum Netzwerk (IP-Adresse u. ä.) gemacht wurden, versucht der Wizard sich mit der

²³ Nessus ist ein Security-Analyser wie Saint oder Satan. Dieses Linux-Tool versucht Schwachstellen in einem System zu finden und aufzudecken.

²⁴ <http://www.pcquest.com/content/hardware/100040101.asp>

²⁵ siehe Anhang J

²⁶ Genauere Informationen hierzu finden sich im Handbuch und in der Firmendokumentation.

nun einzuschaltenden Firebox zu verbinden. Anschließend wird eine Grundkonfiguration übertragen. Nun muss die Verbindung der beiden Netzwerk-Schnittstellen entfernt werden und die WatchGuard entsprechend der Beschaffenheit des Firmennetzwerkes verbunden werden.

- Nun kann die gesicherte Policy von der Management-Station aus eingespielt werden und die Firewall ist wieder voll einsatzfähig.
- Dieser ganze Vorgang wird im Normalfall nicht mehr als 15 Minuten in Anspruch nehmen.

Die von mir eingerichtete Policy-Datei wurde auf eine Diskette gespeichert. Die Diskette befindet sich in einem Umschlag mit der Aufschrift: „Konfigurations-Sicherung 28.03.2001“ und wird mit den übrigen Sicherungsbändern im Tresor aufbewahrt.

Auf der Firebox wurde ein Backup-Image im Flash-RAM erzeugt, sodass auch aus diesem Backup eine Rücksicherung möglich ist.

7 Projektabschluss

7.1 Projektkosten

Zur Berechnung der Gesamtkosten des Projektes werden der investierte Zeitaufwand und die Anschaffungskosten für die neue Firewall herangezogen.

Der von mir als Praktikantin eingebrachte Stundenanteil wird betriebsintern nicht berechnet²⁷. Abteilungsübergreifend wird in der Firma für jeden Mitarbeiter, gleichgültig welcher Stellung, ein fiktiver Stundensatz von 100 DM berechnet. Der Zeitaufwand zweier Mitarbeiter, die bei der Entscheidungsfindung und der späteren Einarbeitung mitwirkten geht daher mit diesem Satz in die Kostenberechnung ein.

Der Investitionsantrag für die WatchGuard Firebox II läuft noch, daher sind hier zurzeit noch keine Kosten entstanden. Zur Einrichtung der Firebox sind keine weiteren Kosten entstanden, da die benötigte Hardware (Kabel, Verbindungstücke, Hub) vollständig im Betrieb vorhanden war oder mit dem Gerät (Netzwerk- und Stromkabel) geliefert wurde. Während des Projektzeitraumes sind zusätzlich Kosten für Telefongespräche bei der Angebotseinholung und in der Testphase, für Kopieren/Ausdrucken von Quell- und Dokumentationsmaterial und für die Internetverbindung der Testumgebung entstanden. Diese Zusatzkosten können nicht genau beziffert werden, sind jedoch auch so geringfügig, dass sie zu vernachlässigen sind.

Aus den genannten Rechnungspositionen ergibt sich die folgende Kosten-Aufstellung:

Projektdurchführung:	1x 35,0 Std.	0,00 DM ²⁸
Entscheidungsgespräch:	2x 1,5 Std.	300,00 DM
Einarbeitung/Übergabe:	2x 1,5 Std.	300,00 DM
(Firebox II laut Angebot:		9.999,00 DM)

Gesamtkosten: 10.599,00 DM

7.2 Rückschau

Mit oder ohne Firewall - vollständige Sicherheit gibt es nicht. Allerdings kann man einiges für die Sicherheit des Netzwerkes machen.

Es ist beeindruckend, wie viele verschiedene Firewallprodukte es auf dem Markt gibt. Dieser Umstand macht deutlich, dass es sich um ein sehr aktuelles Thema handelt. Dabei ist es erstaunlich, wie groß die Preisunterschiede in diesem Bereich sind. Die Definitionen welche Aufgaben eine Firewall hat, unterscheiden sich deutlich voneinander. Es gibt sie als quasi kostenlose Freeware Desktop-Firewalls wie ZoneAlarm, bis hin zu professionellen Lösungen wie der Checkpoint Firewall-1 (Preis je nach Bestandteilen) für mehrere hunderttausend DM. Manche werden als eigenes Gerät in einer Hardware-Box verkauft, andere sind als reine Software zur Installation auf einer bestimmten Plattform erhältlich. Einige verfügen „nur“ über einen reinen Paketfilter (arbeiten also auf Layer 3 und 4) andere haben zusätzlich einen oder mehrere Proxies (bis Layer 7). Es kommt auch vor, dass eine Firewall zusammen mit einem integrierten VPN-Modul, manchmal sogar mit eingebautem Virens Scanner angeboten werden. Dabei gehen die Meinungen darüber, was der Sicherheit zuträglich und was zusätzliches Risiko ist, sehr auseinander. Gelegentlich wird unter einer Firewall nicht nur

²⁷ Ein Auszubildender im dritten Lehrjahr würde in der Firma mit dem Stundensatz von 100 DM arbeiten.

²⁸ Wenn man den Stundensatz eines Azubis zugrundelegt, wären es 3500 DM, die zur Endsumme hinzukämen.

ein System sondern eine ganze Reihe von auf einander abgestimmten kaskadierten Geräten (z.B. die GeNUGate) verstanden. Diese Vielfalt ist vermutlich der steigenden Nachfrage zu verdanken. Allen gemeinsam ist die Aufgabe, den durchgehenden Datenverkehr auf die eine oder andere Weise auf seine Zulässigkeit zu überprüfen.

Die Bedrohung aus dem Internet ist mit der wachsenden Anzahl an privaten Zugängen zum World Wide Web sicherlich stark gestiegen, allerdings wird auch häufig übertrieben, und versucht aus der wachsenden Angst Profit zu schlagen.

Sicherheit ist wichtig. Man sollte sich unbedingt Gedanken über die Sicherheit des Firmennetzwerkes machen und entsprechende Vorkehrungen treffen, dabei aber vermeiden, von der allgemeinen Paranoia mitgerissen zu werden. Eine Firewall wird hier gerne als Allheilmittel gesehen. Sie kann jedoch nur bestimmte Bereiche absichern. Die Sicherheit in einem Unternehmen ist eine ganzheitliche Sache. Sie betrifft das *gesamte* Unternehmen, nicht nur dessen Internetzugang.

Wie aus der Planungstabelle in Kapitel 2 deutlich wird, ist es insgesamt bei den 35 Stunden geblieben. Allerdings weicht der zeitliche Aufwand einzelner Arbeitsschritte von den geschätzten Angaben der Projektplanung ab. Insgesamt ergibt sich dennoch die geplante Anzahl an Arbeitsstunden.

Mit Verlauf und Ergebnis des Projektes war die Firma sehr zufrieden.

7.3 Ausblick

Aus Zeitgründen war es mir im Zuge des Projektes nicht möglich den enormen Funktionsumfang der Firebox II vollständig zu nutzen und alle interessanten Features der Firewall einzurichten.

- Die Einrichtung einer DMZ ist als Folgeprojekt bereits geplant und daher im Netzwerkplan II verzeichnet.
- Zur Nutzung des VPN ist, es noch notwendig entsprechende Zugänge einzurichten und die User mit der Nutzung vertraut zu machen.
- Zur Administration der WatchGuard sollte ein Remote-Zugang eingerichtet werden, sodass bei Abwesenheit der betreuenden Mitarbeiter eine externe Fachkraft diesen Zugang verwenden oder Mitarbeiter das Gerät von Ferne administrieren kann.
- Da das Unternehmen plant, zusätzlich andere europäische Standorte auf die gleiche Weise wie den Niederländischen an das lokale Netzwerk in Bad Zwischenahn anzuschließen, könnte die Einrichtung von VPN-Tunneln zwischen den Standorten und die, mit der Firebox realisierbar, zentrale Firewall-Administration mehrerer Fireboxen interessant werden.

7.4 Dokumentation

Kundengerechte Dokumentation und betriebliche Dokumentation sind für dieses Projekt nicht gesondert angefertigt, da Auftraggeber und Kunde gleich sind. Die Dokumentation aller vorgenommenen Konfigurationen und einige einfache Erläuterungen zur Handhabung der Konfigurationssoftware sind im Anhang I beigelegt. IP-Adressen und andere vertrauliche Informationen wurden aus Sicherheitsgründen entfernt oder anonymisiert, sind allerdings in der Firmendokumentation für den Betrieb vollständig enthalten.

8 Quellennachweis

AS/400 Internet Security Scenarios. Redbooks. Rochester 2000.

Das Grundschutzhandbuch vom BSI (<http://www.bsi.de>)

<http://www.susesecurity.com/faq/>

<http://www.cert.org>

<http://www.ldf.niedersachsen.de>

<http://www.linuxia.de/lt-netfilter.en.html>

<http://netfilter.samba.org/unreliable-guides/netfilter-hacking-HOWTO/index.html>

<http://www.belwue.de/wwwservices/hilfestellungen/ulm/faq/port-num.htm>

Kurtz, McClure, Scambray: Das Anti-Hacker-Buch. Bonn 2000.

RFC 2196 zu finden bei: <http://rfc.fh-koeln.de/rfc/html/rfc2196.html>

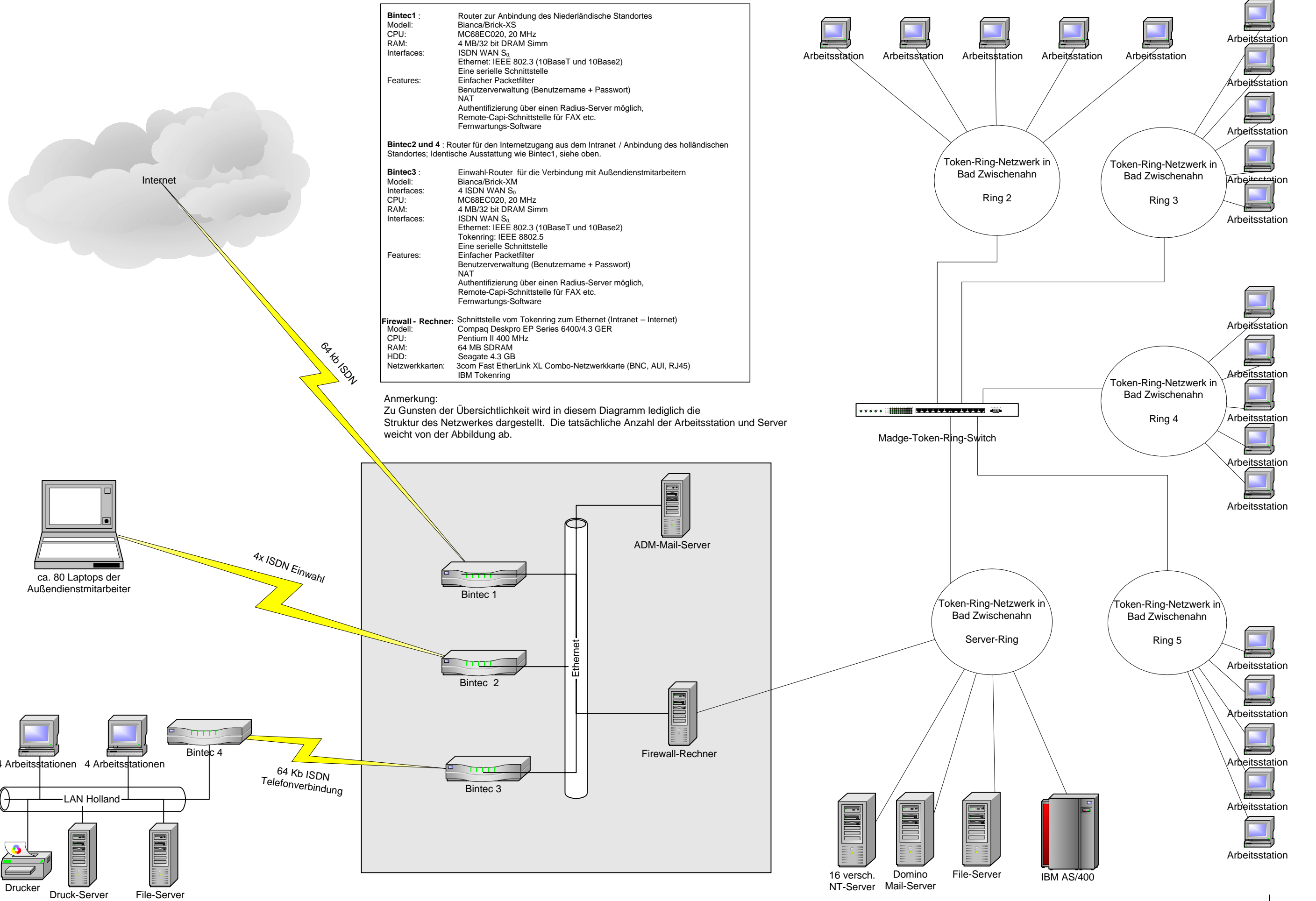
Strobel, Stefan: Firewalls - Einführung, Praxis, Produkte. dpunkt.verlag 1999.

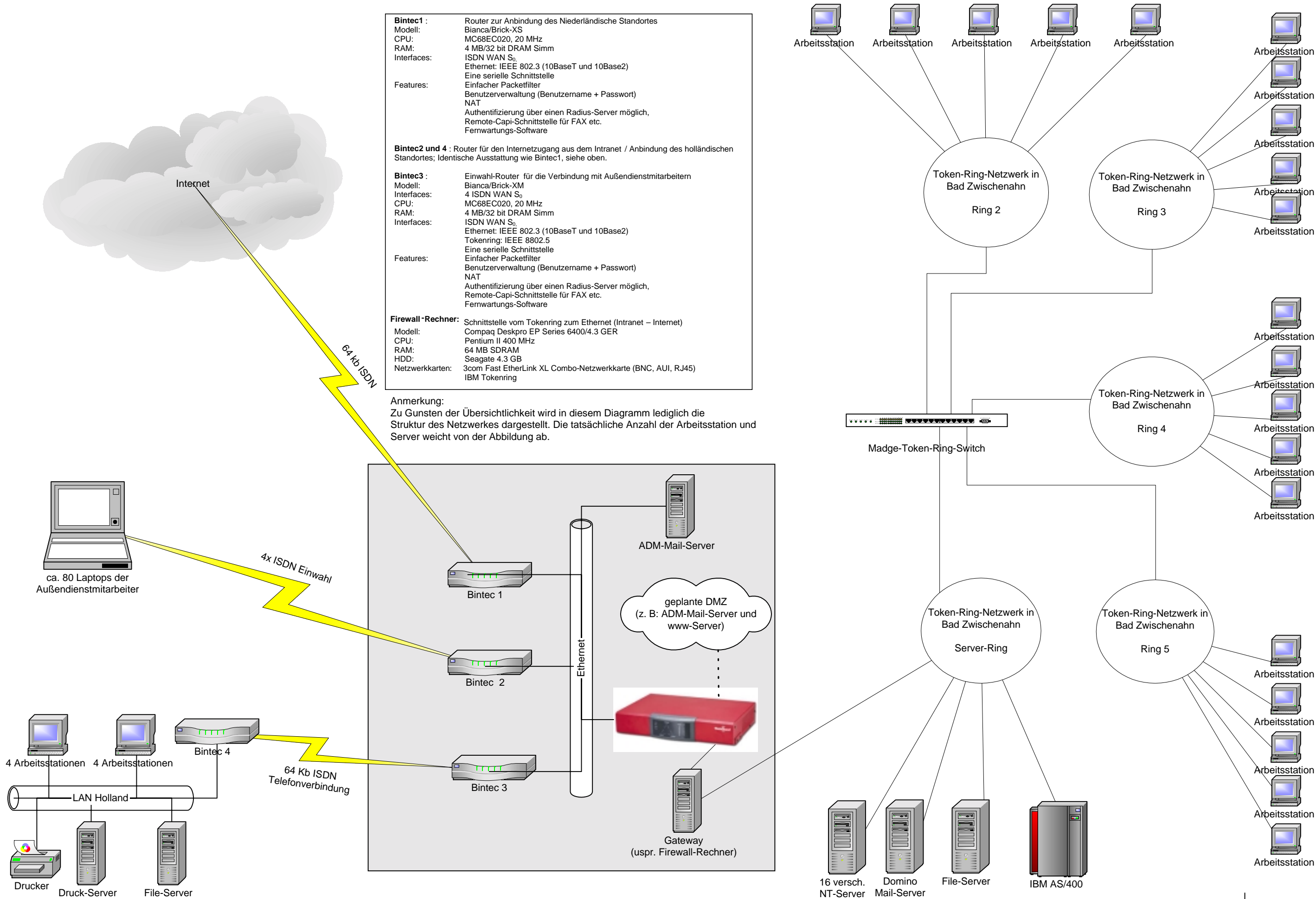
Ziegler, Robert: Linux Firewalls

Zwicky, E. und Cooper, S. : Einrichten von Internet Firewalls. Köln 2001.

9 Anhang

- A. Netzwerkplan I**
- B. Netzwerkplan II**
- C. Das Testsystem**
- D. Konfiguration des Firewall-Rechners**
- E. Leistungsumfang der betrachteten Firewalls (Übersicht)**
- F. Angebote**
- G. Detaillierte Preisübersicht**
- H. Investitionsantrag**
- I. Firmendokumentation**
- J. Nessus Scan Report**
- K. Glossar**





C. Das Testsystem



D. Konfiguration des Firewall-Rechners

Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit. Es sind einige Pakete aufgeführt, die mit Bezug auf den Betrieb einer Firewall interessant sein könnten.

Dienste/Pakete	installiert	im Bootvorgang	nicht gestartet	manuell	Erläuterung
Samba	X	x			Dienst zur Freigabe von Ordnern für Windows-PCs
Ipchains	X	x			Paketfilter-Firewall
Bind	X	X			DNS-Server
Apache	X			X	Web-Server
Squid	X	X			HTTP-Proxy
Sendmail	X	X			Dienst zur Verteilung von E-Mails
Telnet	X	X			Verwaltungs-Werkzeug
Inetd	X	X			Startet Dienste
Ident	x	X			Identifikation
Cron	X	X			Taskmanager
Portmap	X		X		Startet Dienste
NFS	X		X		Dienst für Unix-Freigaben
Routed	X		X		Verteilung von Routing-Informationen
LPD	X		X		Printer Daemon
Ssh	X			X	Secure Shell
X11R6	X		X		X-Server für die grafische Oberfläche
Pop3d	X		X		POP3-Dienst für E-Mail
Imap	X		X		SMTP-Dienst für E-Mail
Saint	X		X		Netzwerk-Analyse-Tool
Wuftp	X		X		FTP-Server
Etherreal	X		X		Netzwerk-Analyse-Tool
John The Ripper	X		X		Passwort-Cracker
Gimp	X		X		Grafikbearbeitung
KDE	X		X		Grafische Oberfläche
Majorhomo	X			X	Mailinglisten unter Linux
cdroast	X		X		CD-Brenner Software
Lynx	X		X		Browser
Mswordview	X		X		Word Viewer
Mtools	X		X		Dos-Tools
Nmap	X		X		Port-Scanner
Rinetd	X				Startet Dienste
Tripwire	X		x		Intrusion Detection-Tool

Die Filterregeln der Firewall wurden mit ipchains umgesetzt. Aus Datenschutzgründen können hier nicht die einzelnen Regeln mit den genauen Quell- und Ziel-Adressen angegeben werden.

Wert	Richtung	Protokoll	Anwendung	Port	Quell-IP	Ziel-IP
Accept	ankommend/ausgehend	TCP	Pflege der E-Mail-Adr.	8383	LAN	Jede
Accept	ankommend/ausgehend	Alles	Programmierer	Jeder	Programmierer	AS/400
Accept	ankommend/ausgehend	TCP	Wartung	telnet	Ext.Firma	RS/6000
Accept	ankommend/ausgehend	TCP	Wartung	ftp-data	Ext.Firma	RS/6000
Accept	ankommend/ausgehend	TCP	MASQ für News	Citrix	PC1	Jede
Accept	ankommend/ausgehend	TCP	MASQ für News	Citrix	PC2	Jede
Accept	ankommend/ausgehend	TCP	MASQ für News	Citrix	PC3	Jede
Accept	ankommend/ausgehend	TCP	MASQ für News	Citrix	PC4	Jede
Accept	ankommend/ausgehend	TCP	MASQ für Citrix-Client	nntp	LAN	Jede
Accept	ankommend/ausgehend	TCP	MASQ für Socks	Socks	PC5	Jede
Accept	ankommend	TCP	Wartung	Smtip	Mail-Relay	Firewall
Accept	ankommend	TCP	Wartung	auth	Mail-Relay	Firewall
Accept	ankommend	TCP	Wartung	Ident	Mail-Relay	Firewall
Accept	ankommend	TCP	Wartung	NetBIOS	File-Server	Mail-Relay
Accept	ankommend/ausgehend	TCP	Wartung	NetBIOS	File-Server	Mail-Relay
Accept	ankommend/ausgehend	alles	Mail-Transfer	Jeder	Notes-Server	LAN
Accept	ankommend/ausgehend	alles	Mail-Transfer	Jeder	Notes-Server	ADM
Accept	ankommend/ausgehend	alles	Wartung	Jeder	RS/6000	Ext. Firma
Accept	ankommend/ausgehend	alles	HüppeNL	Jeder	HüppeNL	AS/400
Accept	ankommend/ausgehend	alles	HüppeNL	Jeder	AdminPC	HüppeNL
Accept	ankommend/ausgehend	alles	HüppeNL	Jeder	HüppeNL	Notes-Server
Accept	ankommend/ausgehend	alles	Router-Verb.	Jeder	Router für NL	AdminPC1
Accept	ankommend	alles	Router-Verb.	Jeder	Router für NL	AdminPC1
Accept	ausgehend	alles	Router-Verb.	Jeder	Router für NL	AdminPC1
Accept	ankommend/ausgehend	alles	Router-Verb.	Jeder	Router für NL	AdminPC2
Accept	ankommend	alles	Router-Verb.	Jeder	Router für NL	AdminPC2
Accept	ausgehend	alles	Router-Verb.	Jeder	Router für NL	AdminPC2
Accept	ankommend	TCP	Router-Konf.	telnet	Bintec1	Firewall-extern
Accept	ankommend/ausgehend	TCP	Router-Konf.	telnet	Bintec1	Firewall-extern
Accept	ausgehend	TCP	Router-Konf.	telnet	Bintec1	Firewall-extern
Accept	ankommend	TCP	Router-Konf.	telnet	Bintec1	Firewall-intern
Accept	ankommend/ausgehend	TCP	Router-Konf.	telnet	Bintec1	Firewall-intern
Accept	ausgehend	TCP	Router-Konf.	telnet	Bintec1	Firewall-intern
Accept	ankommend	Alles	Router-Konf.	Jeder	AdminPC	Bintec1
Accept	ankommend/ausgehend	Alles	Router-Konf.	Jeder	AdminPC	Bintec1
Accept	ausgehend	Alles	Router-Konf.	Jeder	AdminPC	Bintec1
Accept	ankommend	TCP	Mail-Relay-Konf.	ftp-data	Mail-Relay	AdminPC6
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	ftp-data	AdminPC6	Mail-Relay
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	telnet	AdminPC6	Mail-Relay
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	ftp-data	Mail-Relay	AdminPC6
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	NetBIOS	AdminPC6	Mail-Relay
Accept	ankommend/ausgehend	UDP	Mail-Relay-Konf.	ftp-data	AdminPC6	Mail-Relay

Wert	Richtung	Protokoll	Anwendung	Port	Quell-IP	Ziel-IP
Accept	ankommend/ausgehend	TCP	Wartung	ftp-data	Bintec 1	Firewall-intern
Accept	ankommend/ausgehend	TCP	Wartung	telnet	Bintec 1	Firewall-intern
Accept	ankommend/ausgehend	TCP	Wartung	ftp-data	Firewall-intern	Bintec 1
Accept	ankommend/ausgehend	TCP	Wartung	ftp-data	BintecADM	Firewall-intern
Accept	ankommend/ausgehend	TCP	Wartung	telnet	BintecADM	Firewall-intern
Accept	ankommend/ausgehend	TCP	Wartung	ftp-data	Firewall-intern	BintecADM
Reject	ankommend	TCP	Syn-Flag abweisen		Jede	Firewall-extern
Accept	ankommend	UDP	Syslog-UDP	syslog	Bintec 1	Firewall-extern
Accept	ankommend	UDP	Domain	domain	Jede	Firewall-extern
Accept	ankommend	UDP	Samba	NetBIOS	File-Server	Mail-Relay
Accept	ankommend/ausgehend	UDP	Samba	NetBIOS	File-Server	Mail-Relay
Accept	ankommend/ausgehend	TCP	Mail-Relay-Konf.	NetBIOS	AdminPC6	Mail-Relay
Accept	ankommend/ausgehend	UDP	Mail-Relay-Konf.	NetBIOS	AdminPC6	Mail-Relay
Deny	ankommend	UDP	UDP verbieten	Jeder	Jede	Firewall-extern
Deny	ankommend/ausgehend	alles	alles	Jeder	Jede	Jede


E. Leistungsumfang der betrachteten Firewalls

Eigenschaften	SuSE 7.1	Securepoint	Firebox II	Checkpoint	GeNUGate
Paketfilter	ipchains	ipchains	umfangreich, mit vordefinierten Regeln	umfangreich, mit vordefinierten Regeln	eigenes Gerät
Applikation Level	HTTP-Proxy (squid)	HTTP-Proxy (squid)	mehrere Proxies (ohne Cache)	mehrere	mehrere
Windows-Freigaben	Samba-Server	Samba-Client	nein	mit BS möglich	nein
NAT	Masquerading in ipchains	masquerading in ipchains	dynamisch, auch für einzelne Regeln	dynamisch	dynamisch
Interfaces	unbegrenzt	Unterstützt bis zu drei Netzwerkkarten	3x Ethernet 10/100 Mbit	abhängig vom BS	z. B. 2x Ethernet + 1x Token-Ring
IDS	zusätzlich könnte snort installiert/konfiguriert werden	Intrusion Detection System (snort)	einfaches IDS	Umfangreiches IDS	IDS vorhanden
Benutzerverwaltung	eigene Benutzerverwaltung	Eigene Benutzerverwaltung	Eigene, über Radius, NT, CryptoCard, SecureID	Eigene Benutzerverwaltung oder mit LDAP	Eigene Benutzerverwaltung
Log-Dateien	mehrere Dateien in denen die Meldungen gesammelt werden	Umfangreiche Logfiles, die ebenfalls per E-Mail verschickt werden können.	Umfangreiche Logfiles. Auswertung zu Grafiken und Tabellen. Export in Textdatei.	Umfangreiche Logfiles	
Benutzte Sprache	Deutsche Benutzerführung	Deutsche Benutzerführung	englische Benutzerführung	englische Benutzerführung	Deutsche Benutzerführung
Benutzerführung	unübersichtlich	Einfache Installation	Einfache Installation	sehr komplex	vorinstalliert
	in vielen einzelnen Dateien sind Änderungen zu machen	Konfigurationsoberfläche übersichtlich. Einstellungen am Server kompliziert	intuitive Steuerung mit Hilfe von verschiedenen Icons und Menüs	Unübersichtlich, da viele einzelne Module	übersichtlich
	Firewall-Regeln im Textmodus	Grafische Oberfläche zur Regelgestaltung	Regeln in Fenster-Technik konfigurierbar	Grafische Oberfläche zur Regelgestaltung	Konfiguration im Browser
Lizenzen	keine Begrenzung	keine Begrenzung	keine Begrenzung	ab 250 User sehr teuer	bis 500 User
Zeitfenster für Berechtigungen	einstellbar	Zeitfenster auch für die Regelgültigkeit	Zeitfenster auch für die Regelgültigkeit	Zeitfenster auch für die Regelgültigkeit	Zeitfenster auch für die Regelgültigkeit
Webfilter	Dateidownload sperren	Dateidownload sperren	Dateidownload sperren	Dateidownload sperren	Dateidownload sperren
	Sperren von Webseiten	Sperren von Webseiten	Sperren von Webseiten	Sperren von Webseiten	Sperren von Webseiten
		Filtern von Java-Applets	Java, ActiveX, CyberPatrol-Filter	Smart-Filter	externer Filter
VPN	zusätzlich möglich	VPN Modul	VPN mit PPTP, aufrüstbar nach IPsec	VPN gegen Aufpreis	VPN gegen Aufpreis
Updates und Patches	Kostenloses Update auf das nächste Release	Kostenloses Update auf das nächste Release	Updates werden über gesicherte Verbindung zugeschickt. Halbautomatische Installation	Per Post auf CD	Nur mit Wartungsvertrag
Support	Datenbank im Internet	30 Tage-Support	Live Security System	kostenpflichtiger Zusatz	kostenpflichtiger Zusatz
Hersteller	SuSE	Securepoint	WatchGuard (Seattle)	Checkpoint	GeNUA (München)
IP-Adressenfilter	ja	ja	ja	ja	ja
Portfilter	ja	ja	ja	ja	ja
Portforwarding	ja	unbekannt	ja	ja	ja
Durchsatz	voll ausreichend	voll ausreichend	voll ausreichend	voll ausreichend	voll ausreichend
Remote-Zugriff	über telnet	nein	Fernadministrierbar	Fernadministrierbar	Fernadministrierbar
Sonstiges	erweiterbar			stateful inspection	Zwei Rechner in einem Gerät

F. Angebote

+49 421 2020111 5.01

+49 421 2020111



messerknecht-meister
informationssysteme verbinden menschen

Hüppe GmbH & Co.
Duschsysteme
Frau Wiebke Schneider
Industriestraße 3

26158 Bad Zwischenahn

Olaf Timm
Vertrieb
T 0421 / 20 20-347
F 0421 / 20 20-1 11
EMail OTimm@messerknecht.de
OT-Hüppe 14.3.2001

14.3.2001

ANGEBOT

Sehr geehrte Frau Schneider,

wir danken Ihnen für Ihre Anfrage und unterbreiten Ihnen nachstehend auf der Grundlage unserer Allgemeinen Geschäftsbedingungen freibleibend das gewünschte Angebot:

Hardware/Software

Pos.	Anz.	Beschreibung	Einzel-Preis DM	Positions-Preis DM
1.	1	Watchguard Firebox II inkl. 1 Jahr Live Security	10.600,00	10.600,00
2.	1	Verlängerung um 1 Jahr jeweils	1.820,00	
3.	1	Mobile User VPN 50 Clients	6.531,00	
4.	1	Mobile User VPN 100 Clients	12.260,00	
5.	1	Mobile User VPN 250 Clients	24.641,00	

Die Dienstleistungen sind nicht enthalten.

messerknecht-meister informationssysteme GmbH
Sitz Bremen, HRB 6811
Geschäftsführer:
Dipl.-Kfm. Stefan Messerknecht (Sprecher),
Dr. Rainer Bertsch, Dipl.-Betriebswirt Alexander Ruoff

Technologiepark Universität
Linzer Straße 3-5, 28359 Bremen
Postfach 33 03 80, 28333 Bremen
T 0421 / 20 20-0, F 0421 / 20 20-1 11
eMail info@messerknecht.de
http://www.messerknecht.de

it-systeme | software | training | electronic commerce | services

Angebot 1: WatchGuard Firebox II von der Firma Messerknecht-Meister

+49 421 2020111

**messerknecht-meister**
informationssysteme verbinden menschen

Hüppe GmbH & Co.
Duschsysteme Frau Wiebke Schneider
Industriestraße 3, 26158 Bad Zwischenahn

Lieferzeit: nach Vereinbarung

Leistungsort: Leistungsort sind die Räumlichkeiten der
messerknecht-meister informationssysteme GmbH, Bremen

Zahlung: Innerhalb 14 Tagen abzüglich 3% Skonto.
Alle genannten Preise verstehen sich zuzüglich der gesetzlichen Mehrwertsteuer.

Anmerkung: Das Angebot versteht sich vorbehaltlich technischer
Änderungen durch Hersteller und Lieferanten.

Für Rückfragen steht Ihnen Herr Timm gerne zur Verfügung.

Mit freundlichen Grüßen

messerknecht-meister informationssysteme GmbH

Alexander Ruoff

i. A. Olaf Timm

Dieses Angebot wurde maschinell erstellt und ist somit auch ohne rechtsverbindliche Unterschrift gültig.
Auf Wunsch erhalten Sie ein Originalangebot.

it-systeme | software | training | electronic commerce | services

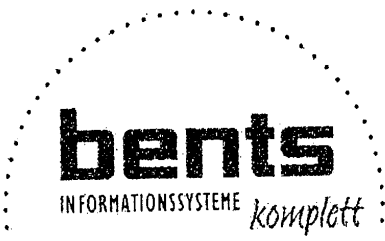
☎ +49 4941 170451	☎ 044038744372	1/3	19.03.2001	12:08	FaxWare
-------------------	----------------	-----	------------	-------	---------

BENTS INFORMATIONSSYSTEME GMBH • LEERER LANDSTRASSE 5-9 •
26603 AURICH

Hüppe GmbH & Co., OHG

z. Hd. Herr Agena
Industriestraße 3

26158 Bad Zwischenahn



BENTS INFORMATIONSSYSTEME GMBH

LEERER LANDSTRASSE 5-9
26603 AURICH
☎ 04941 / 17 04 24
☎ 04941 / 17 04 51

E-MAIL: J.BUSSMANN@BENTS.COM

IHR ZEICHEN, NACHRICHT VOM	UNSER ZEICHEN, NACHRICHT VOM	TELEFON, FAX	DATUM
hüppe/agenta	jobu/bents	Tel.: 04403 / 67 372 Fax: 04403 / 67 44 372	2001-03-19

Angebot

Sehr geehrter Herr Agena,

vielen Dank für Ihre Anfrage.

Wunschgemäß unterbreiten wir Ihnen gemäß unseren allgemeinen Geschäftsbedingungen folgendes Angebot:

MENGE	ARTIKEL	ART-NR.	DM. EINZELPREIS	DM. GESAMTPREIS
1	Watchguard LiveSecurity mit Firebox II Firewall (Hardware) mit Security Management System (SMS) – enthält Remote Office und Branch Office VPN, Historical Reporting, Graphical Monitor, WebBlocker – inkl. 1 Jahr LiveSecurity und WebBlocker-Updates.	EPC1	9.999,00	9.999,00
1	LiveSecurity-Verlängerung FB II Fortlaufende Software-Updates und Patches für 1 Jahr – inkl. WebBlocker-Updates	EPC1	2.189,00	2.189,00
1	LiveSecurity-Verlängerung FB II – 2 Jahre Fortlaufende Software-Updates und Patches für 1 Jahr – inkl. WebBlocker-Updates	EPC1	3.069,00	3.069,00
2	Dienstleistungen: Installation der Firewall, ca. 2 Manntage	Preis pro Manntag	1.250,00	2.500,00

Angebot 2: WatchGuard Firebox II von der Firma Bents



Seite 2 / 3

Lieferung

Die Lieferung erfolgt innerhalb 2 Wochen nach Auftragserteilung. Lieferung erfolgt Frei Haus.

Gewährleistung

Laut unseren Allgemeinen Geschäftsbedingungen 6 Monate Gewährleistung auf von uns gelieferte Produkte und Dienstleistungen. Darüber hinaus gilt die jeweilige Herstellergarantie, wie in den Artikeltexten angegeben. Zusätzlich erforderliche Aufwendungen, insbesondere Transport-, Wege- und Arbeitskosten werden gesondert in Rechnung gestellt.

Zahlbar

Hardware: Nach Erhalt der Rechnung innerhalb 14 Tagen netto Kasse.

Dienstleistungen und Software: Nach Erhalt der Rechnung innerhalb 14 Tagen netto Kasse.

Mehrwertsteuer

Alle Preise verstehen sich zzgl. gesetzlicher Mehrwertsteuer.

Technische Installation

Auf Wunsch erfolgt die technische Installation durch unsere Serviceabteilung. Installationsmaterial wird nach Anforderung des technischen Kundendienstes berechnet, Verkabelungsarbeiten nach erforderlichem Zeitaufwand, zur Zeit 150,- DM pro Stunde.


Anpassungen der Hardware an das Betriebssystem, Installation des Betriebssystems, Organisation der Festplatte, Installation der von uns gelieferten Anwendersoftware wird nach Aufwand berechnet, zur Zeit 150,- DM pro Stunde.

Installationen von Anwendersoftware, die nicht von uns entwickelt wurde, wird ohne Übernahme einer Gewährleistungsverpflichtung auf Wunsch des Auftraggebers durchgeführt. Die Abrechnung erfolgt nach tatsächlichem Zeitaufwand, zur Zeit 150,- DM pro Stunde.

Technischer Kundendienst:

Angebot 2: WatchGuard Firebox II von der Firma Bents

☎ +49 4941 170451	☎ 044038744372	1/3	19.03.2001	12:08	FaxWare
-------------------	----------------	-----	------------	-------	---------



BENTS INFORMATIONSSYSTEME GMBH • LEERER LANDSTRASSE 5-9 •
26603 AURICH

Hüppe GmbH & Co., OHG

z. Hd. Herr Agena
Industriestraße 3

26158 Bad Zwischenahn

BENTS INFORMATIONSSYSTEME GMBH

LEERER LANDSTRASSE 5-9
26603 AURICH

☎ 04941 / 17 04 24
☎ 04941 / 17 04 51

E-MAIL: J.BUSSMANN@BENTS.COM

IHR ZEICHEN, NACHRICHT VOM	UNSER ZEICHEN, NACHRICHT VOM	TELEFON, FAX	DATUM
hüppe/agenta	jobu/bents	Tel.: 04403 / 67 372 Fax: 04403 / 67 44 372	2001-03-19

Angebot

Sehr geehrter Herr Agena,

vielen Dank für Ihre Anfrage.

Wunschgemäß unterbreiten wir Ihnen gemäß unseren allgemeinen Geschäftsbedingungen folgendes Angebot:

MENGE	ARTIKEL	ART-NR.	DM. EINZELPREIS	DM. GESAMTPREIS
1	Watchguard LiveSecurity mit Firebox II Firewall (Hardware) mit Security Management System (SMS) – enthält Remote Office und Branch Office VPN, Historical Reporting, Graphical Monitor, WebBlocker – inkl. 1 Jahr LiveSecurity und WebBlocker-Updates.	EPC1	9.999,00	9.999,00
1	LiveSecurity-Verlängerung FB II Fortlaufende Software-Updates und Patches für 1 Jahr – inkl. WebBlocker-Updates	EPC1	2.189,00	2.189,00
1	LiveSecurity-Verlängerung FB II – 2 Jahre Fortlaufende Software-Updates und Patches für 1 Jahr – inkl. WebBlocker-Updates	EPC1	3.069,00	3.069,00
2	Dienstleistungen: Installation der Firewall, ca. 2 Manntage	Preis pro Manntag	1.250,00	2.500,00

Angebot 2: WatchGuard Firebox II von der Firma Bents



welcome to
the sunny side
of eCommerce

SUNDAY GmbH, Donnerschweer Str. 4, 26123 Oldenburg

Firma

Hüppe GmbH & Co

Frau Wiebke Schneider

Industriestrasse 3

26160 Bad Zwischenahn

Oldenburg, 26.02.2001

Angebot: Firewall Watchguard

Sehr verehrte Frau Schneider,

wie bereits mit Herrn Holz telefonisch besprochen, bieten wir Ihnen hiermit die von Ihnen angefragte Watchguard Firebox II wie folgt an:

1. Firewall

Watchguard Firebox II für bis zu 500 authentifizierten Usern inkl. 1 Jahr Live Security (Subscription) und einem Jahr Hardwaregarantie.	<u>9.578,00 DM</u>
Verlängerung der Subscription inkl. Verlängerung der Hardwaregarantie durch Wick Hill pro weiteres Jahr	<u>2.189,00 DM</u>
Alt. 1. Firebox II plus für 5000 authentifizierten Usern	19.978,00 DM
Alt. 2. Firebox II plus Fast VPN für 5000 authentifizierten Usern und starker VPN Nutzung	27.178,00 DM

2. Installation und Einrichtung

Tagessatz Techniker für Installation und Einrichtung der Firebox nach Kundenwunsch	<u>2.000,00 DM</u>
---	--------------------

3. Schulung

Eintägige Schulung bei Wick Hill in Hamburg. Anfahrt erfolgt auf eigene Kosten	<u>1.800,00 DM</u>
Alternativ Dreitägige Schulung bei Wick Hill in Hamburg inkl. Prüfung, Anfahrt und Unterbringung erfolgt auf eigene Kosten.	<u>3.800,00 DM</u>

4. Fernwartung bzw. Ferndiagnose und Auswertungen

Gerne bieten wir Ihnen auf Wunsch die Fernwartung bzw. Ferndiagnose und Auswertungen der Logfiles der Firebox an. Auf Wunsch führen wir die hierfür nötigen Absprachen mit Ihnen vor Ort in Ihrem Hause durch.

Fon: 0441-98 360 0
Fax: 0441-98 360 29
Internet: www.sunday.de
Email: info@sunday.de

Postbank Hamburg
BLZ 200 100 20, Kto.-Nr. 69 483 207
Kreissparkasse Kirchweyhe
BLZ 291 517 16, Kto.-Nr. 1172

Oldenburgische Landesbank AG
BLZ 280 200 50, Kto.-Nr. 122 38 55 600

Amtsgericht Oldenburg
HRB 4357
Ust-IdNr.:
DE 178 517 474
Geschäftsführer:
Michael Hucke

Angebot 3: WatchGuard Firebox II von der Firma Sunday



welcome to
the sunny side
of eCommerce

Vertragsbedingungen

1. Preisbindung & Abrechnung

Vorbehaltlich zwischenzeitlicher Preisanpassungen und Irrtümer, halten wir uns bis zum 15. März 2001 an dieses Angebot gebunden. Mit diesem Angebot verlieren alle vorhergehenden Angebote ihre Gültigkeit.

Die Preise verstehen sich zzgl. der gesetzlichen Umsatzsteuer.

2. Vertragsschluß & Zahlungsbedingungen

Es gelten die Allgemeinen Geschäftsbedingungen der SUNDAY GmbH für Hardware-Lieferung. Der Vertrag kommt zustande durch die beiderseitig unterschriebene Auftragsbestätigung durch die SUNDAY GmbH.


Sehr verehrter Frau Schneider, wir hoffen, Ihnen ein attraktives Angebot unterbreitet zu haben und freuen uns schon heute darauf, bald von Ihnen zu hören.

Zur Bestellung genügt ein Rückfax mit einer Bestätigung Ihres Bestellwunsches auf diesem Angebot.

Bitte rufen Sie uns an, wenn Sie Fragen haben oder weitere Informationen benötigen.

Fon 0441-98360-0
Fax 0441-98360-29
eMail holz@sunday.de

Mit freundlichen Grüßen


Birger Holz
Angebotswesen / Vertrieb

SUNDAY GmbH

Donnerschwer Str. 4
26123 Oldenburg

Fon +49(441)98360-0 - Fax +49(441)98360-29
--- www.sunday.de ---

Fon: 0441-98 360 0
Fax: 0441-98 360 29
Internet: www.sunday.de
Email: info@sunday.de

Postbank Hamburg
BLZ 200 100 20, Kto.-Nr. 69 483 207
Kreissparkasse Kirchweyhe
BLZ 291 517 16, Kto.-Nr. 1172

Oldenburgische Landesbank AG
BLZ 280 200 50, Kto.-Nr. 122 38 55 600

Amtsgericht Oldenburg
HRB 4357
Ust-IdNr.:
DE 178 517 474
Geschäftsführer:
Michael Hucke

Angebot 3: WatchGuard Firebox II von der Firma Sunday

GeNUA

GeNUA mbH · Räterstraße 26 · D-85551 Kirchheim

Hüppe GmbH & Co
Wiebke Schneider
Industriestraße 3
26160 Bad Zwischenahr

Jörg Seiler
☎ (089) 99 19 50-0
jseiler@GeNUA.DE

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Unser Zeichen: ag-19813

27. Februar 2001

Angebot Nr. ag-19813, GeNUGate Firewallsystem

Sehr geehrte Frau Schneider,

wir bedanken uns für Ihr Interesse und können Ihnen das nachfolgende Angebot unterbreiten.

Dieses Angebot wurde in zwei Abschnitte unterteilt. Variante 1 beinhaltet den einfachen Austausch der vorhandenen Linux-Firewall. Variante 2 umfasst darüber hinaus den Aufbau eines Virtual Private Network (VPN) zwischen dem Hauptstandort und der holländischen Niederlassung.

Als Anlage finden Sie u.a. unsere inzwischen überarbeitete Informationsbroschüre über die GeNUGate Produktfamilie. Mit dem Ihnen im vergangenen Oktober zugegangenen Infopaket haben Sie vermutlich noch eine (inzwischen veraltete) Version dieser Broschüre erhalten.

1. Ausgangssituation

Ihr Unternehmen verfügt über ein Token-Ring-Netz aus rd. 200 Arbeitsplätzen mit einem Internetzugang über eine 64 kBit/s ISDN-Leitung. Dieser Zugang wird bisher durch eine Linux-basierte Firewall abgesichert, die durch ein neues Firewallsystem abgelöst werden soll.

In einem gesonderten Netzsegment (Demilitarisierte Zone – DMZ) sind ein Mailserver sowie zwei ISDN-Router platziert. Über diese Router können sich Mitarbeiter der holländische Niederlassung sowie Außendienstmitarbeiter in das LAN von Hüppe einwählen, um auf dortige Anwendungen zugreifen zu können. Dieses Netzsegment verwendet die Ethernet-Technologie.

An Internetdiensten soll den Anwendern der Webzugriff (HTTP) und das Senden/Empfangen von E-Mails erlaubt sein. Besonderer Wert wird darauf gelegt, den Mitarbeitern keine Downloads zu erlauben.

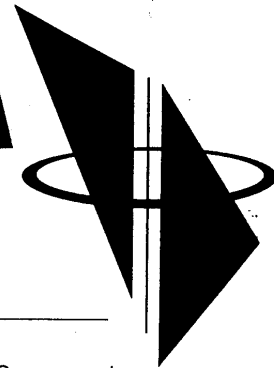
Tel: (089) 99 19 50 – 0
Fax: (089) 99 19 50 – 99
Internet: info@genua.de

Amtsgericht München HRB 98238
Geschäftsführer: Dr. Magnus Harlander,
Dr. Michaela Harlander, Bernhard Schneck

HypoVereinsbank München 4390168840 (BLZ: 700 202 70)
Postbank München 476528808 (BLZ: 700 100 80)
USt-ID: DE129355873

Angebot 4: GeNUGate von der Firma GeNUA

– Seite 2 –

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Ein zentrales Virenscreening auf der Firewall wird nicht gewünscht, da Server und Workstations der Zentrale durch bereits vorhandene Scanner gegen Viren geschützt werden.

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

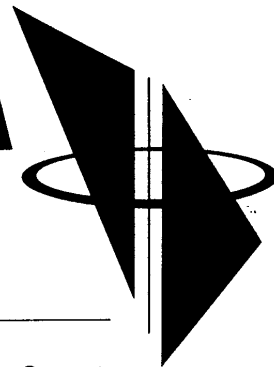
2. Variante 1**2.1 Systemausstattung**

Aufgrund der gewünschten Anforderungen bieten wir Ihnen ein GeNUGate Firewallsystem in der Standardvariante an. Da Applicationlevel Gateway und Paketfilter dieses Systems mit Ethernetkarten ausgestattet sind, wird für den Anschluß an das Token-Ring-LAN eine zusätzliche Token-Ring-Karte nötig. Diese Karte lässt sich gegen die im GeNUGate LAN-seitig vorhandene Ethernetkarte austauschen, die wiederum als Schnittstelle zur vorhandenen Demilitarisierten Zone im Applicationlevel Gateway weiterverwendet werden kann.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
1	1	11431				
GeNUGate Komplettsystem in Standard-Ausstattung						
bestehend aus:						
<i>GeNUGate Server</i> (integriertes Firewall/Serversystem):						
550 MHz AMD K6-2, 512 Kb Cache, 128MB ECC Speicher, 4GB IDE Disk, 2 x 10/100MBit Netzwerkkarten, CDROM, Floppy und VGA Graphik sowie						
<i>GeNUGate Router:</i>						
550 MHz AMD K6-2, 512KB Cache, 32MB Speicher, 2 x 10/100MBit Netzwerkkarten, Floppy und VGA Graphik;						
<i>Gehäuse:</i> 19 Zoll Chassis 4 HE, Netzteil und Lüfter.						
<i>Die Gewährleistungsfrist hinsichtlich der Hardwarekomponenten beträgt abweichend von Par. 17.1. der Allg. Vertragsbedingungen für den Kauf des Systems GeNUGate ein Jahr, gerechnet ab Gefährübergang.</i>						
		€	8666,00	-	-	8666,00
		DEM	16949,22	-	-	16949,22

Fortsetzung auf der folgenden Seite . . .

- Seite 3 -

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
2	1	11226				
		SMC 8115T ISA Tokenring-Karte				
		€	337,00	-	-	337,00
		DEM	659,11	-	-	659,11

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

2.2 Installation

Für die Bestandsaufnahme des vorhandenen Systemumfelds, die Erstellung eines Betriebsfeinkonzepts, die Installation und Konfiguration eines GeNUGate sowie die Einweisung der Firewall-Administratoren in den Gebrauch des Gerätes sind insgesamt zwei Tage zu veranschlagen.

Dieser Zeitbedarf stellt eine Schätzung des Aufwands dar, der für die genannte Tätigkeit aufgrund der uns bekannten Voraussetzungen angesetzt wird. Die Abrechnung erfolgt auf Nachweis der tatsächlich geleisteten Stunden- bzw. Tagessätze.

Ist absehbar, daß der tatsächliche Aufwand den geschätzten Aufwand um mehr als 20 % übersteigen wird, informiert GeNUA Sie rechtzeitig. Dabei gehen wir davon aus, daß die Administratoren bereits allgemeine Kenntnisse im Bereich UNIX-Betriebssysteme, TCP/IP-Netzwerke und Firewall-Technologie besitzen. Auf weitere Schulungsangebote wird weiter unten eingegangen

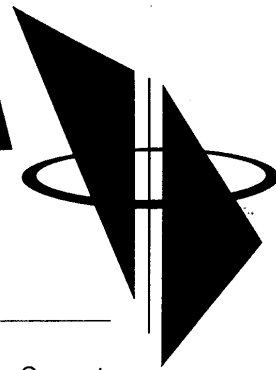
Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
3	2	11846				
		Tagessatz für die Installation, Konfiguration und Einweisung in die Pflege und Benutzung eines GeNUGate Firewallsystems				
		€	1166,00	-	-	2332,00
		DEM	2280,50	-	-	4561,00

2.3 Wartung und Support

Für die Firewalls der GeNUGate-Modellreihe gilt allgemein eine verlängerte Garantiefrist von einem Jahr. Wenn Sie diese Frist weiter ausdehnen möchten, bietet Ihnen GeNUA eine Verlängerung des Garantiezeitraums auf drei Jahre an.

Angebot 4: GeNUGate von der Firma GeNUA

- Seite 4 -

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
4	1	12317				
Hardware-Garantieverlängerung						
Hardware-Garantieverlängerung über das 2. und 3. Jahr für GeNUGate-Systeme mit Standardausstattung.						
Durch diese Garantieverlängerung verlängert sich die Gewährleistung nach Par. 17.1 der Allgemeinen Vertragsbedingungen für den Kauf des Systems GeNUGate hinsichtlich der Hardwarekomponenten auf drei Jahre, gerechnet ab Gefahrübergang.						
			€			
			381,00	-	-	381,00
			DEM			
			745,17	-	-	745,17

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Support für GeNUGate-Software wird von GeNUA in drei Stufen angeboten:

Ein Aktualisierungsservice ist dabei grundsätzlich anzuraten, um auf Dauer den Schutz auch vor neuen Angriffsmethoden zu gewährleisten.

Wenn Sie darüber hinaus auch E-Mail- und Telefonsupport bei unserer Hotline in Anspruch nehmen möchten, wäre für Sie unsere mittlere Supportvariante von Interesse.

Noch weitere Unterstützung hätten Sie durch unseren Systemverwaltungsservice zur Verfügung. Im Rahmen der Systemverwaltung wird von uns ein gesicherter Wartungszugang auf Ihrem GeNUGate eingerichtet, über den wir selbst eventuell anfallende Probleme analysieren und beseitigen können.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
5	1	12364				
GeNUGate Aktualisierungssupport						
Jahresgebühr nur für Aktualisierungen ohne weiteren Support						
			€			
			1963,36	-	-	1963,36
			DEM			
			3840,00	-	-	3840,00
6	1	12386				
GeNUGate Telefon/Emailsupport						
Jahresgebühr für Telefon/Emailsupport inklusive Aktualisierungen						
			€			
			3435,88	-	-	3435,88
			DEM			
			6720,00	-	-	6720,00

Fortsetzung auf der folgenden Seite . . .

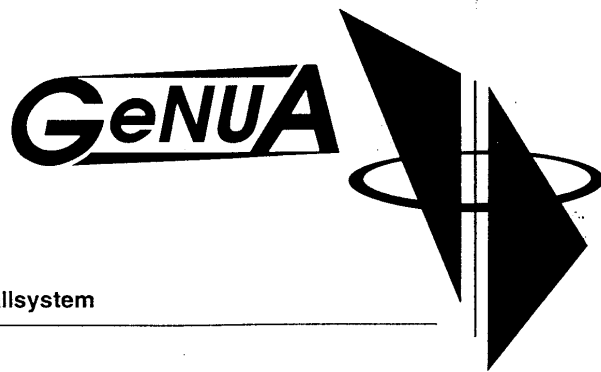
– Seite 5 –

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
7	1	12533				
GeNUGate Systemverwaltungsservice						
Jahresgebühr für Systemverwaltungsservice inklusive Aktualisie-						
rungen						
		€	4755,01	-	-	4755,01
		DEM	9299,99	-	-	9299,99

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

– Seite 6 –



Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Angebot Nr. ag-19813, GeNUGate Firewallsystem

3. Variante 2

3.1 Systemausstattung

Alternativ zu Variante 1 bieten wir Ihnen unser Firewallsystem GeNUGate Pro an. Dieses System unterscheidet sich von GeNUGate nur softwareseitig durch das zusätzliche VPN-Modul auf IPSEC-Basis. Dieses System würde an Ihrem Firmenhauptsitz zum Einsatz kommen.

Als VPN-Gegenstelle würde am holländischen Standort unser Produkt GeNUCrypt installiert. GeNUCrypt beinhaltet ein modifiziertes BSD/OS-Betriebssystem und die komplette VPN-Funktionalität von GeNUGate Pro.

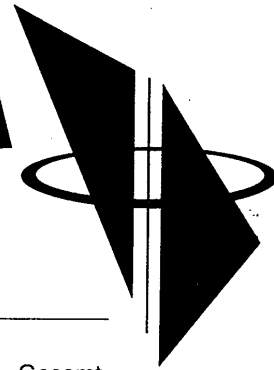
Mit diesen Produkten lässt sich zwischen beiden Standorten ein Layer-3-VPN (volle Netzkopplung) errichten. Detailliertere Informationen zu GeNUCrypt entnehmen Sie bitte der beiliegenden Broschüre über die GeNUGate Produktfamilie.

Der Vorteil von Variante 2 gegenüber Ihrer derzeitigen Situation läge darin, dass der gesamte Datenverkehr zwischen beiden Standorten stark verschlüsselt und mittels Zertifikaten authentisiert würde.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
8	1	11453				
GeNUGate Pro Komplettsystem in Standard-Ausstattung						
bestehend aus:						
<i>GeNUGate VPN-Modul</i>						
<i>GeNUGate Server (integriertes Firewall/Serversystem):</i>						
550 MHz AMD K6-2, 512 Kb Cache, 128MB ECC Speicher, 4GB						
IDE Disk, 2 x 10/100MBit Netzwerkkarten, CDROM, Floppy und						
VGA Graphik sowie						
<i>GeNUGate Router:</i>						
550 MHz AMD K6-2, 512KB Cache, 32MB Speicher, 2 x						
10/100MBit Netzwerkkarten, Floppy und VGA Graphik.						
<i>Gehäuse: 19 Zoll Chassis 4 HE, Netzteil und Lüfter.</i>						
<i>Die Gewährleistungsfrist hinsichtlich der Hardwarekomponenten</i>						
<i>beträgt abweichend von Par. 17.1. der Allg. Vertragsbedingungen</i>						
<i>für den Kauf des Systems GeNUGate ein Jahr, gerechnet ab Ge-</i>						
<i>fahrübergang.</i>						
		€	11223,00	-	-	11223,00
		DEM	21950,28	-	-	21950,28

Fortsetzung auf der folgenden Seite ...

- Seite 7 -

GeNUA

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Angebot Nr. ag-19813, GeNUGate Firewallsystem

Pos	Anz	ArtNr		Einzelpreis	Zu/Abschl	Betrag	Gesamt
9	1	11226					
			SMC 8115T ISA Tokenring-Karte				
			€	337,00	-	-	337,00
			DEM	659,11	-	-	659,11
10	1	14088					
			GeNUCrypt Hardware				
			bestehend aus: <i>GeNUGate Router.</i>				
			Celeron 700MHz, 64MB RAM, 2 x 10/100MBit Netzwerkkarten,				
			CDROM, Floppy und VGA Graphik.				
			<i>Gehäuse:</i>				
			19 Zoll Chassis 2 HE, Netzteil und Lüfter.				
			<i>Die Gewährleistungsfrist hinsichtlich der Hardwarekomponenten beträgt abweichend von Par. 17.1. der Allg. Vertragsbedingungen für den Kauf des Systems GeNUGate ein Jahr, gerechnet ab Gefahrübergang.</i>				
			€	1610,00	-	-	1610,00
			DEM	3148,89	-	-	3148,89
11	1	11860					
			GeNUCrypt				
			IPSEC-Router-Software inkl. Betriebssystem				
			€	2556,00	-	-	2556,00
			DEM	4999,10	-	-	4999,10

Zur gesicherten Einwahl externer Mitarbeiter bieten wir Ihnen die Software von F-Secure an. Dabei handelt es sich um die kommerzielle Variante der Secure Shell SSH.

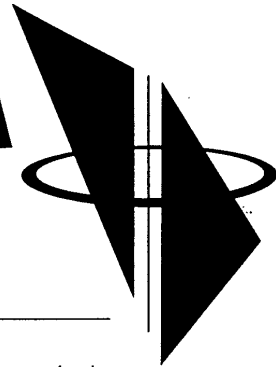
Auf dem Firewallsystem kommt dabei der SSH-Server zum Einsatz (eine modifizierte Variante des kommerziell erhältlichen F-Secure-Servers für Unix), während auf den PCs der externen Mitarbeiter die F-Secure-Clientsoftware installiert wird. Die Clientsoftware ist für Windows-, Macintosh- und UNIX-Rechner erhältlich.

Mittels der F-Secure-Software wird eine gesicherte Verbindung aufgebaut, bei der die beiden beteiligten Rechner sich gegenseitig authentisiert haben und deren Datenstrom mittels kryptographisch starker Algorithmen mit mindestens 128 Bit Schlüssellänge verschlüsselt ist. Durch Port Forwarding lassen sich dann über die F-Secure-Verbindung weitere TCP-Verbindungen tunneln, sofern deren Portnummern bekannt sind.

Die Software kann auf den Clients so installiert und konfiguriert werden, daß der Aufbau der F-Secure-Verbindung mittels einfachen Mausklicks erfolgt.

Der Unterschied zu dem obigen (Layer-3-)VPN-Modul besteht darin, dass die SSH-

- Seite 8 -

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Anbindung keine volle Netzkopplung bietet. Für Außendienstmitarbeiter können in der Regel nicht die gleichen Sicherheitsregeln eingehalten werden wie innerhalb eines Firmennetzes. Daher wird meist gewünscht, daß Außendienstmitarbeiter nur auf die für ihre Tätigkeit notwendigen Anwendungen zugreifen dürfen.

Als zusätzliche Sicherheit für die Anbindung von Außendienstmitarbeitern ist die Authentisierung mittels Einmalpasswörtern per S/key-Verfahren oder CryptoCard (Preis auf Anfrage) möglich. Damit lassen sich die enormen Sicherheitsrisiken für das LAN, die z.B. bei Verlust eines Laptops entstehen würden, deutlich verringern.

Das Angebot enthält zwei Mengenstaffeln der F-Secure-Clientsoftware; weitere Staffeln können wir Ihnen auf Anfrage gerne nennen.

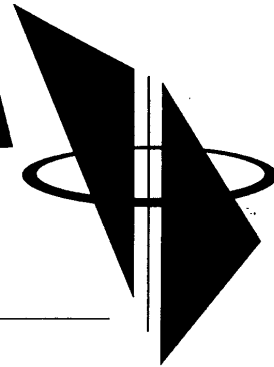
Wir möchten Sie darauf hinweisen, dass neben der kommerziellen Version der Client-Software von F-Secure auch die Möglichkeit besteht, auf den Client-Rechnern freie Software wie z.B. die OpenSSH-Software einzusetzen. Dabei ist darauf zu achten, dass die Clients mit dem SSH 1-Protokoll betrieben werden und die Möglichkeit des Port-Forwardings bieten.

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Pos	Anz	ArtNr		Einzelpreis	Zu/Abschl	Betrag	Gesamt
12	1	12230					
		F-Secure Server					
		Serverlizenz für GeNUGate					
		€	795,00	-	-	795,00	
		DEM	1554,88	-	-	1554,88	
13	1	12151					
		F-Secure Client					
		Paketpreis 25er Lizenz					
		€	3472,00	-	-	3472,00	
		DEM	6790,64	-	-	6790,64	
14	1	12162					
		F-Secure Client					
		Paketpreis 50er Lizenz					
		€	6672,00	-	-	6672,00	
		DEM	13049,30	-	-	13049,30	

Angebot 4: GeNUGate von der Firma GeNUA

– Seite 9 –

GeNUA

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Angebot Nr. ag-19813, GeNUGate Firewallsystem

3.2 Installation

Durch die zusätzlich notwendige Installation und Konfiguration von GeNUCrypt ist in dieser Variante mit insgesamt 3 Tagessätzen zu rechnen. Vergleichen Sie dazu bitte unsere Erläuterungen zu Punkt 2.2.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
15	2	11846				
		Tagessatz für die Installation, Konfiguration und Einweisung in die Pflege und Benutzung eines GeNUGate Firewallsystems				
		€	1166,00	-	-	2332,00
		DEM	2280,50	-	-	4561,00
16	1	13073				
		Tagessatz Seniorberater:				
		Installation und Konfiguration von GeNUCrypt				
		€	1165,75	-	-	1165,75
		DEM	2280,01	-	-	2280,01

3.3 Wartung und Support

Wie in Variante 1 bieten wir Ihnen für GeNUGate Pro die Verlängerung des Garantiezeitraums auf 3 Jahre an. Für GeNUCrypt-Hardware existiert diese Möglichkeit derzeit nicht.

– Seite 10 –

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
17	1	12317				
Hardware-Garantieverlängerung						
Hardware-Garantieverlängerung über das 2. und 3. Jahr für GeNUGate-Systeme mit Standardausstattung.						
Durch diese Garantieverlängerung verlängert sich die Gewährleistung nach Par. 17.1 der Allgemeinen Vertragsbedingungen für den Kauf des Systems GeNUGate hinsichtlich der Hardwarekomponenten auf drei Jahre, gerechnet ab Gefahrübergang.						
		€	381,00	-	-	381,00
		DEM	745,17	-	-	745,17

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Ähnlich wie für GeNUGate (s. Punkt 2.3) existieren für GeNUGate Pro Systeme 3 unterschiedliche Supportvarianten. Der höhere Preis ergibt sich durch das zusätzliche VPN-Modul.

Für GeNUCrypt existieren zwei Supportvarianten.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
18	1	12375				
GeNUGate Pro Aktualisierungssupport						
Jahresgebühr nur für Aktualisierungen ohne weiteren Support						
		€	2760,98	-	-	2760,98
		DEM	5400,01	-	-	5400,01
19	1	12397				
GeNUGate Pro Telefon/Emailsupport						
Jahresgebühr für Telefon/Emailsupport inklusive Aktualisierungen						
		€	4233,50	-	-	4233,50
		DEM	8280,01	-	-	8280,01
20	1	12522				
GeNUGate Pro Systemverwaltungsservice						
Jahresgebühr für Systemverwaltungsservice inklusive Aktualisierungen						
		€	5798,05	-	-	5798,05
		DEM	11340,00	-	-	11340,00

Fortsetzung auf der folgenden Seite . . .

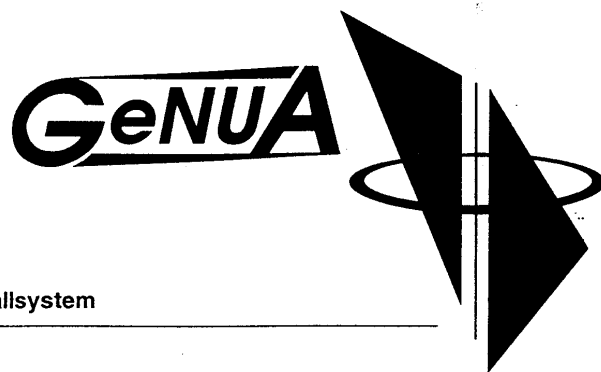
- Seite 11 -

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
21	1	13332				
		GeNUCrypt Aktualisierungssupport				
		Jahresgebühr nur für Aktualisierungen ohne weiteren Support				
		€	511,29	-	-	511,29
		DEM	1000,00	-	-	1000,00
22	1	13343				
		GeNUCrypt Telefon/Emailsupport				
		Jahresgebühr für Telefon/Emailsupport inklusive Aktualisierungen				
		€	766,94	-	-	766,94
		DEM	1500,00	-	-	1500,00

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

- Seite 12 -



Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Angebot Nr. ag-19813, GeNUGate Firewallsystem

4. Schulung

GeNUA bietet ihren GeNUGate-Kunden drei aufeinander aufbauende Schulungskurse für den Betrieb dieser Firewall an:

Der UNIX und TCP/IP-Kurs vermittelt die notwendigen Betriebssystem- und Netzwerk-Kenntnisse.

Der GeNUGate-Einführungskurs wendet sich an Firewall-Administratoren, die ein GeNUGate in einfachen Umgebungen betreuen wollen.

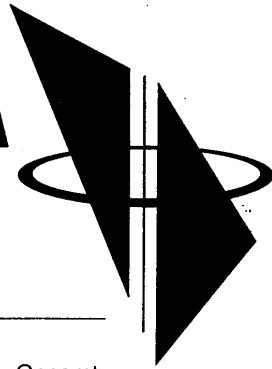
Der Interna-Kurs ist für fortgeschrittene Firewall-Administratoren geeignet, die ein GeNUGate in komplexeren Umgebungen einsetzen oder ein *Virtual Private Network* (VPN) mit einem GeNUGatePro betreiben wollen und dafür Einblick in die GeNUGate-Interna benötigen.

Genauere Informationen über die Schulungsinhalte entnehmen Sie bitte der beiliegenden Schulungsbroschüre.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
23	1	13206				
Schulung Unix und TCP/IP						
Dauer: 1 Tag – Ort: Schulungsraum bei GeNUA						
Inhalt: grundlegendes Wissen über Unix und TCP/IP						
		€	787,00	-	-	787,00
		DEM	1539,24	-	-	1539,24
24	1	12915				
Schulung GeNUGate-Einführung						
Dauer: 1 Tag – Ort: Schulungsraum bei GeNUA						
Inhalt: Grundlagen zu Firewallsystemen, Systemaufbau, Features, Einsatzumgebung, Administration						
		€	787,00	-	-	787,00
		DEM	1539,24	-	-	1539,24

Fortsetzung auf der folgenden Seite . . .

- Seite 13 -

GeNUA**Angebot Nr. ag-19813, GeNUGate Firewallsystem**

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
25	1	13952				
Schulung GeNUGate-Interna						
für Administratoren mit fundiertem Firewallwissen.						
Dauer: 3 Tage – Ort: Schulungsraum GeNUA						
Inhalt: Grundlagen zu Firewallsystemen und TCP/IP, Systemaufbau, GeNUGate-Interna, Konfiguration der Dienste, Kommunikationswege, Integration in komplexe Netze, Paketfilter, besondere Sicherheitsfeatures, Immutable Flags, GUI, Manuelle Konfiguration, Lokale Erweiterungen, Format und Funktion der Registry, Performancefragen, Ausfallsicherheit, Funktion des Basisbetriebssystems BSD/OS, Remote-Access, VPN						
			€			2531,00
			DEM			4950,21

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

5. Security-Newsletter

Als wertvolle Hilfe für den Firewall-Administrator, der über das aktuelle Gefährdungspotential auf dem laufenden bleiben will, bieten wir unseren GeNUA Security-Newsletter an. Damit informieren wir unsere Kunden über neu bekanntgewordene und von uns verifizierte Sicherheitsprobleme und ersparen ihnen dadurch die Notwendigkeit, die einschlägigen Newsgruppen und Mailinglisten selbst zu verfolgen.

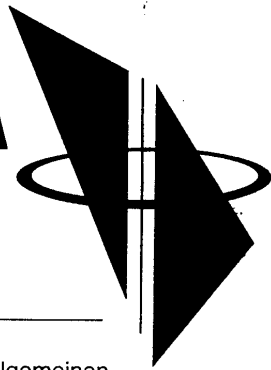
Weitere Informationen finden Sie auf unserem Webserver¹. Gerne schalten wir Ihnen auch ein vierwöchiges Probeabonnement frei. Wenden Sie sich dazu bitte formlos an info@genua.de.

Pos	Anz	ArtNr	Einzelpreis	Zu/Abschl	Betrag	Gesamt
26	1	13040				
GeNUA Security-Newsletter						
Laufende aktuelle Meldungen zu sicherheitsrelevanten Themen von der GeNUA-Newsletter-Redaktion; Jahresabonnement						
			€			613,55
			DEM			1200,00

¹<http://www.genua.de/produkte/newsletter/index.html>

– Seite 14 –

GeNUA



Angebot Nr. ag-19813, GeNUGate Firewallsystem

Für unsere Lieferungen und Leistungen gelten die nachfolgenden Allgemeinen Geschäftsbedingungen:

- Die Allgemeinen Vertragsbedingungen für die Pflege von Software (beigefügt).
- Die Allgemeinen Vertragsbedingungen für den Kauf des Systems GeNUGate (beigefügt).
- Die Teilnahmebedingungen für GeNUGate-Schulungen (auf der Rückseite der Schulungsinformation abgedruckt).
- Die Bezugsbedingungen für den Security-Newsletter (beigefügt).

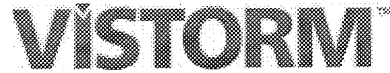
Das Angebot ist bis zum 27.03.2001 gültig!

Mit freundlichen Grüßen,

Jörg Seiler
Vertrieb

Gesellschaft für
Netzwerk- und UNIX-
Administration mbH

Vistorm GmbH
Tel: +44 1925 66 56 56
Fax: +44 1925 66 72 04
Email: lars-helge.lund@vistorm.com
www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/1

Sehr geehrte Frau Schneider!

Mit Bezug auf unser Gespräch am Montag 16/02-2001 sende ich wie angefordert den Vorschlag von Vistorm GmbH für eine VPN Lösung mit Managed Service

Vistorm ist führend in der Bereitstellung verwalteter Firewall- und Virtual Private Network- (VPN-) Security-Lösungen und -Services und verwaltet momentan einige der größten FireWall-1 und Internet-VPN-Einsätze in Europa. Vistorm ist der Partner mit den höchsten Akkreditierungen von Check Point Software Technologies und ein Security Partner für UUNET. Vistorm ist in einer einzigartigen Position, die höchsten Serviceniveaus anzubieten, indem die große Erfahrung und bescheinigte technische Sachkenntnis unseres rund um die Uhr geöffneten, sicheren Network Operations Centre verwendet wird.

Die Einzelheiten zu unserem Kostenvoranschlag finden Sie umseitig. Falls Sie Fragen haben oder weitere Informationen benötigen, können Sie mich gerne unter folgender Telefonnummer erreichen: +44 (0) 1925 66 56 56.

Mit freundlichen Grüßen

Lars Lund

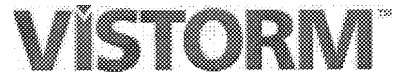
Vistorm GmbH
Quattrium,
Kaiserswerther Strasse 115
40880 Ratingen
Germany

Tel: +49 (0)2102 560 9800
Fax: +49 (0)2102 560 9899

Vistorm Limited
Vistorm house,
3200 Daresbury Park, Daresbury
WA4 4BU
England

Tel: +44 (0) 1925 66 56 56
Fax: +44 (0) 1925 66 72 04

Vistorm GmbH
Tel: +44 1925 66 56 56
Fax: +44 1925 66 72 04
Email: lars-helge.lund@vistorm.com
www.vistorm.com

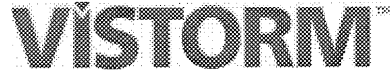


Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/2

Einhalt

EINLEITUNG	3
SCHRITTE	3
VORAUSSETZUNGEN.....	3
OPTIONEN	3
KOSTENVORANSCHLAG	4
CHECK POINT	4
NOKIA	4
UUNET	4
CHECK POINT-PREISE <i>SCHRITT 1</i>	5
CHECK POINT-PREISE <i>SCHRITT 2</i>	5
CHECK POINT SECUREREMOTE	6
CHECK POINT FIREWALL-1 <i>ALTERNATIVE LÖSUNG</i>	6
NOKIA-PREISE <i>SCHRITT 1</i>	7
NOKIA-PREISE <i>SCHRITT 2</i>	7
UUNET BUDGET-PREISE <i>SCHRITT 1</i>	8
ÜBERSICHT UUNET BUDGET-PREISE <i>SCHRITT 2</i>	8
VISTORM™ -PREISE <i>SCHRITT 1</i>	9
VISTORM™ -PREISE <i>SCHRITT 2</i>	10

Vistorm GmbH
Tel: +44 1925 66 56 56
Fax: +44 1925 66 72 04
Email: lars-helge.lund@vistorm.com
www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/3

Einleitung

Wie vereinbart, senden wir Ihnen einen Kostenvoranschlag für die Sicherung von Bad Zwischenahn. Der Kostenvoranschlag beruht auf den unten genannten Schritten, Voraussetzungen und Optionen. Angabe über einzelne Preise für alle hier aktuellen Produkte finden Sie nach Hinten. Für die UUNET Preise bitten wir Sie das beigelegte Dokument von UUNET durchzugehen.

Schritte

Zwei Schritte werden vorgeschlagen. Erstens wird Bad Zwischenahn, den Sie als 2Mb definiert haben, mit den notwendigen Softwares, Hardwares, Unterstützung und Verwaltung ausgestattet.

Der zweite Schritt bietet eine vollständige VPN Lösung für die 6 Standorte, mit den kompletten Softwares, Hardwares, Unterstützung und Verwaltung. Die einzelnen Preise für Software und Hardware in Schritt 2 müssen wir später besprechen, aber wir haben ein Beispiel für max 25 Benutzer pro Standort gemacht.

Voraussetzungen

Wir setzen folgendes voraus, dass das Angebot ein komplettes Paket ist, das ohne Rücksprache nicht verändert werden kann.

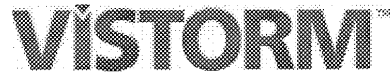
Nur eine DMZ wird vorgeschlagen für den Standort Rheinau aber dies ist erweiterbar.

UUNET/ISP: Bitte notieren Sie sich, dass dies NUR Budget Preise sind.

Optionen

Wie vereinbart bekommen Sie Preise für das Nokia Advanced Replacement, wie Sie wissen bietet Nokia optionelle Alternativen z.B. 8x5- und 24x7 an. In der Zusammenfassung werden Lösungen von Vistorm vorgeschlagen, die Vistorm in verschiedenen Fällen für notwendig hält, z.B. empfehlen wir für Bad Zwischenahn mindestens 256K bit Linie und 128K bit für die 5 andere Standorte. Tiered Service, wie vorgeschlagen für Bad Zwischenahn, bedeutet das Sie bekommen ein 2M bit Linie aber Sie wählen selbst, wie viel Sie benutzen möchten, z.Bs. können Sie innerhalb 24 Stunden die Linie von 256K bit bis 2M bit erweitern.

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/4

Kostenvoranschlag

Schritt 1			Schritt 2		
Estimation of costs for 1-Site Gateway Service			Estimation of costs for 5-Sites VPN Service		
	Set-Up	Service		Set-Up	Service
Software	10,328.00	1,551.00	Software	13,560.00	2,040.00
Hardware	6,114.00	1,046.00	Hardware	15,410.00	2,250.00
ISP	1,274.00	13,682.00	ISP	10,624.66	82,795.84
Vistorm Management	17,700.00	27,100.00	Vistorm Management	12,000.00	31,300.00
Total	35,416.00	43,379.00	Total	51,594.66	118,385.84

Die Auswahl an Produkten und Services von Vistorm für Managed Internet Security-Lösungen stellt sicher, dass unsere Kunden das höchste Niveau an verfügbarer technischer Sachkenntnis erhalten. Vistorm hat sich dazu entschlossen, nur mit solchen Produzenten eine Partnerschaft einzugehen, die beste Spitzentechnologie entwickeln. Das Unternehmen wurde von allen unseren ausgewählten Partnern: Check Point Software Technologies Certified Managed Service Provider und Premier Partner, OPSEC Alliance Partner, Nokia Strategic Partner und UUNET UK Security Partner, mit dem höchsten Akkreditierungsniveau ausgezeichnet.

Check Point

Vistorm ist der einzige Premier Partner von Check Point, der die gesamte Produktpalette von Check Point unterstützt:

- FireWall-1: Die einzige echte zur Verfügung stehende Enterprise Security Firewall-Architektur.
- VPN-1: Virtual Private Network-Lösung, die auf FireWall-1 basiert. Bietet Algorithmen, die IPsec entsprechen sowie eine einfache Handhabung.

NOKIA

Vistorm bietet das gesamte Sortiment der NOKIA Router-Lösungen an. Diese enthalten FireWall-1 und bieten dem Benutzer eine Black-Box-Lösung. Diese Systeme sind entwickelt worden, um eine hohe Leistungsfähigkeit, zusätzliche Sicherheit und Zuverlässigkeit zur Verfügung zu stellen. Auch die Möglichkeit, eine hoch verfügbare FireWall-1 bereitzustellen, ist enthalten, so dass die Firewall trotz einem Hardware- oder Softwareversagen aktiv bleibt.

UUNET

Vistorm kann durch UUNET, dem weltweit größten Internet Service Provider, Verbindung zum Internet anbieten. Vistorm kann das gesamte Sortiment der UUNET-Lösungen anbieten und als ersten Kontakt für den Support aller Ihrer Internet- und VPN-Anforderungen agieren.

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/5

Check Point-Preise Schritt 1

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Network Security-Software				
1	1	Check Point VPN-1 v4.1 <ul style="list-style-type: none"> VPN-1 Module für Unlimited Benutzer Medien und Dokumentation 	€ 10,328.00	€ 10,328.00

Check Point VPN-1 v4.1 Unterstützung				
2	1	12 Monate Softwarewartung – Upgrades für Unlimited Benutzer <ul style="list-style-type: none"> Alle größeren und kleineren Software, Medien- und Dokumentations-Upgrades 	€ 1,551.00	€ 1,551.00

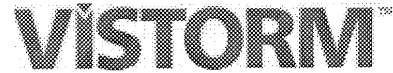
Check Point-Preise Schritt 2

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Network Security-Software				
3	5	Check Point VPN-1 v4.1 <ul style="list-style-type: none"> VPN-1 Module für 25 Benutzer Medien und Dokumentation 	€ 2,712.00	€ 13,560.00

Check Point VPN-1 v4.1 Unterstützung				
4	5	12 Monate Softwarewartung – Upgrades für 25 Benutzer <ul style="list-style-type: none"> Alle größeren und kleineren Software, Medien- und Dokumentations-Upgrades 	€ 408.00	€ 2,040.00

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
 Voranschlagsnummer: LL200201WS/6

Check Point SecureRemote

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Check Point Secure Remote Software				
5		Check Point VPN-1 SecureRemote Software	€ 0.00	€ 0.00

Secure Remote bekommt man Kostenlos, man muss nur die Lizenzen registrieren

Check Point Firewall-1 Alternative Lösung

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Network Security-Software				
6	1	Check Point FW-1 v4.1 • FW-1 Enterprise Center (Unlimited Benutzer) * • Medien und Dokumentation	€ 22,488.00	€ 22,488.00
7	1	Encryption Add on für Unlimited Benutzer	€ 4,616.00	€ 4,616.00
			Gesamtpreis für die Alternative L.	€ 27,104.00

Check Point VPN-1 v4.1 Unterstützung				
8	1	12 Monate Softwarewartung – Upgrades • Alle größeren und kleineren Software, Medien- und Dokumentations-Upgrades	€ 4,068.00	€ 4,068.00

* Wählen Sie das Managed Service benötigen Sie keinen Enterprise Center

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com

VISTORM™

Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/7

Nokia-Preise Schritt 1

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
Nokia Network Security-Hardware				
9	1	Nokia IP330 System <ul style="list-style-type: none"> System mit 256mb RAM Nokia Routing System Drei Port Ethernet 10/100 PCI-Schnittstelle IPSO Software und System-Dokumentation Stecker- und Spannungssatz für Deutschland 	€ 6,114.00	€ 6,114.00

Nokia IP330 Wartung				
10	1	Software Subscription <ul style="list-style-type: none"> Nokia IP Betriebssystem-Upgrades Technische Unterstützung Übersendung von Ersatzteilen am nächsten Geschäftstag 	€ 1,046.00	€ 1,046.00

Nokia-Preise Schritt 2

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
Nokia Network Security-Hardware				
11	5	Nokia IP110 System <ul style="list-style-type: none"> System mit 64mb RAM Drei Port Ethernet 10/100 PCI-Schnittstelle IPSO Software und System-Dokumentation Stecker- und Spannungssatz für Deutschland 	€ 3,082.00	€ 15,410.00

Nokia IP110 Wartung				
12	5	Software Subscription <ul style="list-style-type: none"> Nokia IP Betriebssystem-Upgrades Technische Unterstützung Übersendung von Ersatzteilen am nächsten Geschäftstag 	€ 450.00	€ 2,250.00

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com

VISTORM™

Kostenvoranschlag für: Hüppe GmbH & Co
 Voranschlagsnummer: LL200201WS/8

UUNET Budget-Preise Schritt 1

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

UUNET Internet-Verbindung				
13	1	UUNET Set-up Leased Line – 2M bit	€ 1,274.00	€ 1,274.00
14	1	12 Monate UUNET 256M bit Tiered Service (Max 2M bit) <ul style="list-style-type: none"> • 64Kb PS bis 2Mb PS Glasfaserstandleitung • Unbegrenzte Netzwerkverwendung • Speichern und Weiterleiten von E-mails • Primary DNS (<30 Hosts) • 12 Monate 24-stündige technische Unterstützung u. SLA 	€ 13,682.00	€ 13,682.00

Übersicht UUNET Budget-Preise Schritt 2

Site	Linie			Euro Converter**		
	Bandbreite	Set-up	Monatlich	conv.	Set-up	Jährlich
1 Deutschland	2M bit	2,490.00 DM	4,990.00 DM	0.51128	1,273.09	30,615.45
2 Polen*	144K bit	2,000.00 zł	1,595.00 zł	0.26572	531.44	5,085.88
3 Belgien	128K bit	164,910.00 BF	42,283.00 BF	0.02478	4,086.47	12,573.27
4 Niederlande	128K bit	fl 5,050.00	fl 2,565.00	0.45377	2,291.54	13,967.04
5 Spanien	128K bit	406,343.00 Pts	285,000.00 Pts	0.00601	2,442.12	20,554.20
PS! Nur Budget Preise, sehen Sie auch beigelegte Dokumente von UUNET				Total	10,624.66	82,795.84

* Teleco-setup und -jährliche Kosten fehlt für Polen
 ** Nur zu Vergleich

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/9

Vistorm™ -Preise Schritt 1

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Vistorm Managed Gateway Service				
15	1	FireWall-1 Managed Internet Security Setup – 1 Firewalls <ul style="list-style-type: none"> • Alle benötigten Beratungen, um die Sicherheitspolice von unseren Sicherheitsexperten zu analysieren und einzurichten. • Die Police ist auf den Kunden angepasst und erstellt, um genaue Sicherheitsanforderungen zu erfüllen. • Aufbau der Regelgrundlagen für jedes Firewall-Modul und jedes -Gateway. • Projektleitung • Ferne Ausführung der Policen aller Firewall-Module und -Gateways. • Option: Einrichten von bis zu 200 Benutzern in der FireWall-1-Benutzerdatenbank. • Hinweise zu Meldungs- und Fallreaktion. Teilnummer: MSFW1-1-SU	€ 17,700.00	€ 17,700.00
			Gesamtpreis Set-up	€ 17,700.00

Vistorm Managed Gateway Service				
16	1	FireWall-1 Managed Internet Security Service – 1 Firewalls <ul style="list-style-type: none"> • 12 Monate vollständig verwalteter Service für Check Point FireWall-1 • Fernverwaltung der Firewalls von geschulten CCSE's 24 Stunden am Tag, 365 Tage im Jahr • Technische Unterstützung für benannte Kontaktpersonen per Hotline • Bis zu 12 administrative Änderungen pro Jahr an Regeln, Zielen, Services, Address Translation und Routing • Formale Änderungskontrollverfahren • Option: SecuRemote Management • Option: Ausführliche Berichte • Formale Meldungs- und Antwortverfahren • Proaktiver Rat und proaktive Verwaltung • Option: Bis zu 200 Änderungen pro Jahr an der Benutzerdatenbank • Ausführung der Software-Patches und -Upgrades • Vollständig gesichertes Network Operation Centre (NOC) 	€ 27,100.00	€ 27,100.00
			Gesamtpreis Service	€ 27,100.00

Vistorm GmbH
 Tel: +44 1925 66 56 56
 Fax: +44 1925 66 72 04
 Email: lars-helge.lund@vistorm.com
 www.vistorm.com



Kostenvoranschlag für: Hüppe GmbH & Co
Voranschlagsnummer: LL200201WS/10

Vistorm™ -Preise Schritt 2

Artikel	Menge	Produktbeschreibung	Stückpreis	Gesamtpreis
---------	-------	---------------------	------------	-------------

Vistorm Managed VPN Service				
17	5	FireWall-1 Managed Internet Security Setup – 5 Firewalls <ul style="list-style-type: none"> • Alle benötigten Beratungen, um die Sicherheitspolice von unseren Sicherheitsexperten zu analysieren und einzurichten. • Die Police ist auf den Kunden angepasst und erstellt, um genaue Sicherheitsanforderungen zu erfüllen. • Aufbau der Regelgrundlagen für jedes Firewall-Modul und jedes – VPN-Gateway. • Projektleitung • Ferne Ausführung der Policen aller Firewall-Module und -Gateways. • Einrichten von bis zu 200 Benutzern in der FireWall-1-Benutzerdatenbank. • Hinweise zu Meldungs- und Fallreaktion. Teilnummer: MSFW1-5-SU	€ 2,400.00	€ 12,000.00
			Gesamtpreis Set-up	€ 12,000.00

Vistorm Managed VPN Service				
18	5	FireWall-1 Managed Internet Security Service – 5 Firewalls <ul style="list-style-type: none"> • 12 Monate vollständig verwalteter Service für Check Point FireWall-1 • Fernverwaltung der Firewalls von geschulten CCSE's 24 Stunden am Tag, 365 Tage im Jahr • Bis zu 5 administrative Änderungen pro Jahr an Regeln, Zielen, Services, Address Translation und Routing • Formale Meldungs- und Antwortverfahren • Proaktiver Rat und proaktive Verwaltung • Ausführung der Software-Patches und –Upgrades • Vollständig gesichertes Network Operation Centre (NOC) 	€ 6,260.00	€ 31,300.00
			Gesamtpreis Service	€ 31,300.00

G. Detaillierte Preisübersicht

Kosten für Variante 1 (SuSE 7.1 Firewall) im Einzelnen:

1. Das **Betriebssystem** SuSE Linux 7.1 Professionell ist bei jedem Softwarevertrieb zu kaufen. Der Preis ist weder firmenabhängig noch an eine bestimmte Anzahl von Benutzern gebunden. Der Karton beinhaltet 7 CDs und eine DVD. Weitere Softwareprodukte müssen für den Betrieb der Firewall nicht hinzu erworben werden.
Software (von Logibyte): 129,00 DM
2. **Hardware:**
 Das Firewall-System wird auf einem Standard Compaq-Rechner installiert, da dieser für den Betrieb der Firewall geeignet erscheint. Es handelt sich dabei um zuverlässige Markengeräte, deren Leistungsvermögen (CPU, Speicher ...) für die Anforderungen der Linux-Firewall mehr als ausreichend ist.
Für einen Compaq-Rechner: 2000,00 DM
3. Linux ist ein sehr komplexes Betriebssystem, das keinem der Mitarbeiter vollständig vertraut ist. Zudem verwenden auch potentielle Angreifer eines Netzwerkes häufig dieses Betriebssystem, das sie bestens kennen und manipulieren können. Es werden immer wieder neue Lücken aufgedeckt, die es zu beseitigen gilt. Da zur Einrichtung und Wartung einer Firewall auf die Sicherheit des Systems großen Wert gelegt werden sollte, erscheint eine gute Grundlagen**Schulung** wenigstens eines Mitarbeiters sinnvoll.
 Eine entsprechende Schulung bietet die Firma IFTT Consult in München, Bonn oder Frankfurt an. Sie besteht aus zwei Teilen:
 Schulung eines Firmenmitarbeiters:
 Theorie: 3395,00 DM
 Praxis: 2795,00 DM
Gesamt: 6220,00 DM
4. Die **Installation** der Hardware und des Linux-Betriebssystems mit Einrichtung aller erforderlichen Treiber wird ca. 3 Arbeitsstunden beanspruchen. Hinzu kommt nach erfolgter Einrichtung die Integration in das Netzwerk, was ca. 1 Stunde erfordert. Als Stundensatz werden nach Angaben der Personalabteilung 100 DM fällig.
 Einrichtung: 4 x 100,00 DM
Gesamt: 400,00 DM
5. Die eigentliche **Konfiguration** der Firewall mit Übernahme bzw. Anpassung aller bisherigen Einstellungen der jetzigen Firewall wird voraussichtlich ca. 8 Arbeitstunden beanspruchen. Diese Angabe ist jedoch grob geschätzt.
 Bei einem Stundensatz von wiederum 100 DM ergeben sich:
 Einrichtung/Konfiguration: 8 * 100,00 DM
Gesamt: 800,00 DM
6. Das CERT meldet fast täglich neu Schwachstellen in Linux-Systemen. Das bedeutet nicht, dass Linux ein besonders lückenhaftes Betriebssystem ist, sondern nur, dass es besonders ausgiebig untersucht und getestet wird. Allerdings ist es ratsam, sich darüber regelmäßig zu informieren und bekannt gewordene Schwachstellen zu beseitigen. Die Distributoren stellen zu diesem Zweck meist ziemlich schnell entsprechende Updates und Patches zur Verfügung. Die **Wartung** eines Linux-Systemes erfordert jedoch wöchentliche Pflegearbeiten von ca. 1 Stunde Aufwand.
 Arbeitsstunden pro Jahr: 52 Wochen * 1 Arbeitsstunden
 Stundensatz: 100,00 DM
 Wartung pro Jahr: 52 Stunden * 100,00 DM
Gesamt: 5200,00 DM

Insgesamt ergeben sich für Variante 1 damit folgende Kosten für
 das erste Betriebsjahr: 14689,00 DM
 Kosten für jedes weitere Jahr: 5200,00 DM
 für die ersten drei Jahre: 25089,00 DM

*Kosten für Variante 2 im Einzelnen:***Checkpoint Firewall 1:**

- Die Firewall1-Software kann auf verschiedenen Plattformen installiert werden. Vistorm bietet als **Betriebssystem und Hardware** ein Nokia IP330 System an. Diese Hardware und das Betriebssystem sind austauschbar. Andere Produkte bietet Vistorm jedoch nicht an, und diese wurden aus zeitlichen Gründen in diesem Projekt auch nicht weiter berücksichtigt. Das Gerät ist in mehreren Versionen verfügbar. Sie unterscheiden sich durch ihre hardwareseitige Leistungsfähigkeit. Auf Grund der Leistung kommt das Nokia IP330 System in Frage.
Hardware + OS: 12228,00 DM
- Die eigentliche **Firewall-Software** kann mit oder ohne Management-Konsole bestellt werden. Wird die Software ohne das Management-Modul erworben, so kann die Wartung nicht selbstständig durchgeführt werden. Da wir die Konfiguration der Firewall aus Kostengründen betriebsintern vornehmen möchten, muss die Firewall1-Software über eine Management-Konsole verfügen.
Firewall-1-Software + Management-Konsole: 74864,00 DM
- Die **Einrichtung** kann auf Grund der Komplexität nach Angaben des Resellers nur vom Fachmann durchgeführt werden. Der Vertragspartner bietet die Einrichtung zu einem Gesamtpreis von 35400,00 DM an. Je nach Aufwand können diese Angaben jedoch stark variieren.
Es wurde vom Vertreiber ein Tagessatz von ca. 4000 DM genannt
Einrichtung/Konfiguration: 35400,00 DM
- Ein so häufig eingesetztes Produkt wie die Checkpoint wird ständig auf Sicherheitslücken untersucht. Entsprechende Updates und Patches stellt die Firma jedem lizenzierten Betreiber einer Firewall-1 schnellstmöglich zur Verfügung. Diese sollten vor Ort in das System eingespielt werden, um es aktuell zu halten. Der **Subscription-Service** wird vom Vertragspartner auf 12 Monate berechnet.
Firewall1-Subscription: 8136,00 DM
Nokia-Subscription: 2092,00 DM
Gesamt: 10228,00 DM
- Notwendige Updates und Patches müssen wie bereits erwähnt eingespielt werden, in regelmäßigen Abständen sollten die Log-Dateien auf Auffälligkeiten untersucht werden. Allerdings ist das IDS-System der Checkpoint in der Lage bekannte Angriffsmuster selbständig zu erkennen und zu melden. Nach Angaben des Anbieters wird die **Wartung** der Checkpoint durchschnittlich 2 Stunde pro Monat in Anspruch nehmen. Bei einem Stundensatz von 100 DM ergibt sich folgende Berechnung:
Wartung: 12 Monate * 2h * 100 DM
Gesamt: 2400,00 DM

Insgesamt ergeben sich für die Checkpoint damit folgende Kosten für

das erste Betriebsjahr: 135120,00 DM

jedes weitere Jahr fallen weiterhin Kosten an: 2400,00 DM

10228,00 DM

Für die ersten drei Betriebsjahre: 160374,00 DM

WatchGuard:

- Die WatchGuard ist eine feste **Hard- und Software-Kombination**. Da mir diese Firewall aufgrund ihres vergleichsweise guten Kosten-Nutzen-Verhältnisses besonders interessant erschien, wurden hier mehrere Angebote eingeholt. Je nach Reseller variieren die Preise um einige Hundert DM.
Firma Sunday: 9578,00 DM
Firma Bents: 9999,00 DM
Firma Messerknecht-Meister: 10600,00 DM
- Die einjährige Garantie für das Gerät und das LiveSecuritySystem kann, unabhängig vom Reseller, verlängert werden. Dies erscheint mir für eine Firma wie Hüppe (Endkunde mit eigener EDV-Abteilung) recht sinnvoll, da die Wartung einer Firewall umfangreiches Fachwissen und auch ständige Aufmerksamkeit erfordert. Mit dem LiveSecuritySystem kommen Updates und Informationen zur Sicherheit quasi von allein ins Haus und es wird eine 24h Hotline zur Verfügung gestellt. Diese Verlängerung kommt allerdings erst **ab dem zweiten Jahr** zum Tragen, da die genannten Leistungen für das erste Betriebsjahr bereits im Preis unter Punkt 1 enthalten sind.
Garantie/Subscription-Verlängerung pro Jahr:

- | | |
|---------------------|-------------------|
| Firma Sunday: | 2189,00 DM |
| Firma Bents: | <u>2189,00 DM</u> |
| Firma Messerknecht: | 1820,00 DM |
3. Da die WatchGuard sich laut Vertreter durch besonders einfache und übersichtliche Benutzerführung auszeichnet, wird von der betriebsinternen **Einrichtung** der Firebox II ausgegangen. Der Zeitaufwand hierfür ist nur recht ungenau einzuschätzen, daher wird zur Berechnung an dieser Stelle der gleiche Zeitaufwand wie für die SuSE-Firewall angenommen.
Bei einem Stundensatz von wiederum 100 DM ergeben sich:
- | | |
|----------------------------|------------------|
| Einrichtung/Konfiguration: | 8 * 100,00 DM |
| <u>Gesamt:</u> | <u>800,00 DM</u> |
4. Auch die WatchGuard muss wie jede andere Firewall-Lösung regelmäßig gepflegt werden, allerdings ist der notwendige Aufwand weitgehend automatisiert. Beispielsweise werden Updates auf einer gesicherten Verbindung automatisch über das Internet geschickt. Der Administrator wird an seiner Arbeitsstation davon benachrichtigt. Für die Untersuchung der Log-Dateien und das eventuell notwendige Einpflegen neuer Konfigurationen bleibt noch ein Arbeitsaufwand von ca. 2h pro Monat. Wie bei den vorherigen Berechnungen wird für die Arbeitszeit ein Stundensatz betriebsintern von 100 DM berechnet.
- | | |
|-----------------|-------------------------|
| Wartung: | 12 Monate * 2h * 100 DM |
| <u>Gesamt:</u> | <u>2400,00 DM</u> |

Insgesamt ergeben sich für die Firebox II beim Zugrundelegen der Preise von Bents damit folgende Kosten für das erste Betriebsjahr: 13199,00 DM
jedes weitere Jahr fallen weiterhin Kosten an: 2189,00 DM
2400,00 DM
Insgesamt für die ersten drei Jahre: 22377,00 DM

GeNUGate

1. Die GeNUGate ist wie die WatchGuard eine feste **Hard- und Software**-Kombination. Sie kann in drei Varianten bestellt werden, welche sich durch ihre Leistungsfähigkeit unterscheiden. Für Hüppe kommt die GeNUGate Pro mit extra VPN-Modul in Betracht, da die Firma in naher Zukunft VPN einsetzen möchte, und das günstigere Standardprodukt nicht über diese Funktion verfügt. Grundsätzlich soll das Produkt also über eine VPN-Option verfügen. Zusätzlich für den VPN-Betrieb notwendige Bestandteile werden zu diesem Zeitpunkt aber noch nicht berücksichtigt und müssen später nachgerüstet werden. Zur Integration der Firewall in das Token-Ring-Netz kann eines der drei Netzwerk-Interfaces gegen Aufpreis als Token-Ring-Netzwerkkarte bestellt werden.
- | | |
|---------------------------|--------------------|
| Hard- und Software: | 21950,28 DM |
| Token-Ring-Netzwerkkarte: | 659,11 DM |
| <u>Gesamt:</u> | <u>22609,39 DM</u> |
2. Der Hersteller bietet eine **Hardware-Garantieverlängerung** für bis zu drei Jahre an.
Garantieverlängerung pro Jahr: 745,17 DM
3. **Aktualisierungen der Software** und sonstige Supportleistungen sind in drei Stufen unterteilt. Der einfache Aktualisierungssupport beinhaltet nur die Softwareupdates, Telefon/E-Mailsupport ermöglicht darüber hinaus entsprechende Anfragen, und auf diesem Wege Hilfestellungen bei Problemen; der Systemverwaltungsservice bietet einen Komplettservice. Die Preise beziehen sich auf 12 Monate.
- | | |
|-------------------------------|-------------------|
| Aktualisierungssupport: | 5400,01 DM |
| <u>Telefon/E-Mailsupport:</u> | <u>8280,01 DM</u> |
| Systemverwaltungsservice: | 11340,00 DM |
4. Die **Einrichtung** der GeNUGate muss laut Anbieter von einem fachkundigen Mitarbeiter durchgeführt werden. Die Dienstleistung umfasst die Installation, Konfiguration und Einweisung der Firewall. Sie beinhaltet noch nicht die Einrichtung des VPN.
Es wird ein Tagessatz von 2280,50 DM berechnet. Der Anbieter kalkuliert für diese Arbeit zwei Arbeitstage.
Installation/Einrichtung: 4561,00 DM

5. Da der Telefon/E-Mailsupport gewählt wurde, muss der Aufwand für die regelmäßige Wartung der Firewall bedacht werden. Den Angaben des Herstellers zur Folge, könnte der hier ein ähnlicher Aufwand zu Grunde gelegt werden, wie bei der WatchGuard oder Checkpoint.

Wartung: 12 Monate * 2h * 100 DM

Gesamt: 2400,00 DM

Insgesamt ergeben sich für die GeNUGate damit folgende Kosten:

Für das erste Betriebsjahr: 38595,57 DM

Jedes weitere Jahr fallen weiterhin Kosten an: 11425,18 DM

Insgesamt für die ersten drei Jahre: 61445,93 DM

Securepoint

1. Die Securepoint kann als reines **Software-Paket** oder im Bundle mit passender **Hardware** erworben werden. Da für den Einsatz dieses Produktes ohnehin ein eigener Computer angeschafft werden müsste, wird hier von einer Bundle-Lösung ausgegangen.

Bundle 1 : 4199,00 DM

2. Die **Installation** der Securepoint dauert ca. 20 Minuten¹. Die Weboberfläche zur **Konfiguration** ist nicht sehr umfangreich, und daher entsprechend schnell zu konfigurieren (ca. 60 Minuten). Mit Integration in das Netzwerk und Testphase kommen für die **Einrichtung** einer Securepoint vielleicht 4 Arbeitsstunden² zusammen.

Installation/Einrichtung: 4 * 100 DM

Gesamt: 400 DM

3. Die Securepoint muss wie jede andere Firewall-Lösung regelmäßig gepflegt werden. Updates müssen eingespielt werden. Log-Dateien müssen untersucht werden. Das, plus das eventuell notwendige Einpflegen neuer Konfigurationen wird mit einem Arbeitsaufwand von ca. 2h pro Monat kalkuliert. Wie bei den vorherigen Berechnungen wird für die Arbeitszeit ein Stundensatz betriebsintern von 100 DM berechnet.

Wartung: 12 Monate * 2h * 100 DM

Gesamt: 2400,00 DM

Insgesamt ergeben sich für die Securepoint damit folgende Kosten für

das erste Betriebsjahr: 6999,00 DM

jedes weitere Jahr fallen weiterhin Kosten an: 2400,00 DM

Insgesamt für die ersten drei Jahre: 11799,00 DM

¹ Angabe des Herstellers

² Angabe des Herstellers

Investitionsantrag

Technische Beschreibung des Investitions-Gegenstandes:

Die Aufgabe einer Firewall besteht darin, das Unternehmensnetzwerk mit all den darin enthaltenen Daten gegen unerwünschte, eventuell schädliche Zugriffe von außen zu schützen. Die Watchguard Firebox II ist eine dem aktuellen Stand der Technik entsprechende Hardware-Firewall. In diesem Gerät ist die verwendete Hardware genau auf die installierte Software abgestimmt. Im Einzelnen beinhaltet die Investition folgende Hard- und Software-Bestandteile:

Hardware:

- 200 MHz Pentium MMX Prozessor
- 64 MB SDRAM
- 8 MBFlash-Ram
- 3 RJ-45 10/100 Ethernet Interfaces

Software:

- Spezielles Betriebssystem
- Konfigurations-Software
- LiveSecuritySystem

Sonstiges:

- Regelmäßige Updates der Software

Begründung des Antrages:

Die gespeicherten Daten eines Unternehmens sind sein Kapital. Um eventuell irreparablen Schaden zu vermeiden, müssen diese Daten so gut wie möglich geschützt werden. Firmennetzwerke werden in ständig zunehmendem Maße aus dem Internet angegriffen. Dabei werden Internetzugänge der Unternehmen lahmgelegt oder für illegale Machenschaften missbraucht. Daten werden zerstört oder wie im jüngsten Falle bei Microsoft gestohlen. Kleinere und mittelständische Unternehmen sind hiervon ebenso betroffen wie die größeren. Solche Attacken haben unterschiedliche Hintergründe: Es kann Industriespionage dahinter stehen, aber auch Neugier, Wettkampf zwischen Hackern oder einfach Zerstörungswut. Für die betroffenen Unternehmen bedeutet dies häufig irreparablen Schaden und Verdienstausschlag.

Bisher wird das Firmennetzwerk von Hüppe durch eine Linux-Firewall geschützt. Diese Firewall ist nun einige Jahre alt. Da sich die Angriffstechniken der Eindringlinge ständig wandeln, muss eine entsprechende Schutzvorrichtung laufend angepasst werden. Die von uns favorisierte Form der Aktualisierung besteht in dem Ersatz der Linux-Firewall durch die oben vorgestellte Watchguard-Firebox II.

Folgende Gründe sprechen für diese Lösung:

Verminderter Zeitbedarf bei der notwendigen Pflege der Firewall durch:

- vereinfachte Installation der Updates
- durch LiveSecurity keine Suche nach Sicherheitslücken und den zugehörigen Updates
- Sicherheitslücken werden von der Firma Watchguard aufdecken und beseitigt.

Verbesserte Sicherheit durch:

- einfach durchschaubare Regeln
- ein spezialisiertes System, dass sich beschränkt auf die Funktionen einer Firewall
- sichere, weil verschlüsselte Übertragung der Updates
- kompetente Ansprechpartner und Entwickler
- Einsatz eines kommerziellen Webfilters; Vermeiden von Schmutz-Webseiten im Unternehmen
- Verbesserte Eindringlingserkennung

Zusätzlich bietet die Watchguard folgende Möglichkeiten:

- VPN (virtuelle private Netzwerke)
- Die Datenübertragung kann nach aktuellem Standard verschlüsselt werden.
- Zusätzliche spezielle Filtermöglichkeiten
- Authentifizierung an der Firewall
- Kommerzieller Web-Filter
- Teilweise automatisierte Eindringlingserkennung und -abwehr

Kostenersparnis:

- weniger Zeitbedarf (Wartung, Web-Filter)
- Verbindungen über Internet (mit VPN) statt Telefon

Investitionskosten:

Je nach Anbieter variieren die zu veranschlagenden Kosten. Der von uns favorisierte Anbieter ist die Firma Bents aus Aurich, die uns bereits ein Gerät zum Test zur Verfügung gestellt hat.

Firebox II + LiveSecurity für 1: 9999,00 DM

LiveSecurity-Verlängerung auf zwei Jahre: 2189,00 DM

Insgesamt: 12188,00 DM



**DOKUMENTATION ZUR
WATCHGUARD-FIREBOX II**



Von: Wiebke Schneider
Erstellt am: 29.03.2001

Inhaltsverzeichnis

1	AUFBAU DER FIREBOX	2
1.1	STANDORT IM NETZWERK	2
1.2	KABELVERBINDUNGEN	2
1.3	FIREBOX ZURÜCKSETZEN	2
2	INSTALLATION DER LIVE SECURITY SOFTWARE	3
3	FIREBOX GRUNDLAGEN	3
3.1	FIREBOX-VOREINSTELLUNGEN	3
3.2	KOMMUNIKATION MIT DER FIREBOX	3
3.3	DIE LIVESECURITYSOFTWARE	4
3.3.1	Control Center	4
3.3.2	Policy Manager	5
3.3.3	Firebox Monitor	5
3.3.4	LogViewer	6
3.3.5	HostWatch	7
3.3.6	Historical Reports	7
3.3.7	LiveSecurity Inbox (BackWeb)	8
4	SETUPWIZARD	9
5	EINSTELLUNGEN	13
5.1	IP-ADRESSEN	13
5.2	AUTHENTIFIZIERUNG	14
5.3	PAKETFILTER UND PROXIES	15
5.4	LOGGING	18
5.5	PASSWÖRTER	18
6	WARTUNG	18
7	NOTFALLPLAN	19
7.1	SICHERUNGSDISKETTE	19
7.2	FALL: FEHLERHAFTE KONFIGURATION	19
7.3	FALL: PASSWORT VERGESSEN	19
7.4	FALL: UPDATE FEHLGESCHLAGEN	20
7.5	FALL: FIREBOX NICHT MEHR ERREICHBAR	20

1 Aufbau der Firebox

1.1 Standort im Netzwerk

Die Firebox hat drei Ethernet-Netzwerkschnittstellen.

Eine Schnittstelle, die als External Interface bezeichnet wird und mit dem Router bzw. in unserem Fall mit dem Ethernet verbunden wird.

Eine zweite Schnittstelle wird als Internal Interface bezeichnet. Diese stellt die Verbindung zum Lokalen Netzwerk dar und wird bei uns mit dem Inthuepp1 verbunden.

Die dritte heißt Optional Interface. Diese ist für den Einsatz von verschiedenen aus dem Internet zugänglichen Servern (z.B. Webservern, Mail-Servern, Ftp-Servern, ...) gedacht. Hier könnte zum Beispiel in unserem Falle der Mail-Server stehen.

Sie sollte physikalisch zwischen dem Internet und dem LAN eingesetzt werden, sodass eine Verbindung nur über die Box hergestellt werden kann.

Die Workstation von der aus die Konfiguration vorgenommen werden soll, muss nicht im gleichen logischen Netzwerk eingerichtet werden.

Beide Geräte (Firebox und Management-Workstation) sollten in einem gesicherten Bereich betrieben werden, damit unbefugter Zugriff nicht möglich ist.

1.2 Kabelverbindungen

Mit der Firebox werden vier Kabel mitgeliefert.

Das rote Netzwerkkabel ist zum direkten Anschluss des external Interface an den Router gedacht und daher gedreht. Dieses Kabel wird in unserem Fall hier nicht verwendet, da das external Interface der Firebox mit einem Hub in das Ethernet integriert wird. Das external Interface sollte also mit einem Standard Netzwerkkabel an den Ethernet-Hub angeschlossen werden.

Die zwei grünen Netzwerkkabel sind ganz normale Standard-TP-Netzwerkkabel der Kategorie 5. Sie sind zum Anschluss des trusted/optional Interface an das LAN bzw. das optionale Netzwerk gedacht, können aber beliebig als Netzwerkkabel eingesetzt werden. In unserem Fall wird die WatchGuard am trusted Interface mit einem roten Crossover Kabel an den Inthuepp1 angeschlossen. Auf diese Weise kann ein zusätzlicher Hub eingespart werden.

Das blaue Kabel ist ein serielles Kabel. Mit diesem Kabel kann eine lokale Verbindung zur Firebox aufgebaut werden, falls die Konfiguration nicht über das Netzwerk erfolgen soll.

Weitere Informationen hierzu finden sich auch im InstallGuide auf Seite 12.

1.3 Firebox zurücksetzen

Die Firebox kann auf ihre Standard-Einstellungen zurückgesetzt werden, falls notwendig.

Achtung: Alle Konfigurationseinstellungen der Firebox gehen dabei verloren. Diese müssen nachträglich (z.B. von einer Sicherungsdiskette) neu implementiert werden.

Hierzu verbindet man die Managment Workstation über das trusted Interface oder das serielle Kabel mit der Firebox und schließt zwei der drei Netzwerkschnittstellen der Firebox für die folgende Konfiguration mit dem roten Cross-Over-Kabel kurz. Dann schaltet man die Firebox aus und wieder an. Die Firebox bootet dann im Fail-Safe-Modus (Standard-Einstellungen ab Werk). Diese wird von den LEDs durch das flackernde „SysA“ angezeigt.

Nun startet man den Setup-Wizard und verbindet sich auf diese Weise mit der Firebox. Dabei wird eine einfache Standard-Policy erzeugt. Auch die Passwörter werden dabei neu gesetzt.

Nach Beendigung des Setup-Wizard muss das Cross-Over-Kabel entfernt werden.

Mit Hilfe des Policy-Managers kann nun die alte, hoffentlich gesicherte , Konfigurations-Datei (*.cfg) übertragen werden. Auf diese Weise ist in wenigen Minuten die gesicherte Konfiguration wieder hergestellt.

2 Installation der Live Security Software

Die CD einlegen und warten bis der Willkommens-Dialog erscheint. Die Installation ist selbsterklärend und kann im Prinzip auf jedem beliebigen WindowsNT- oder Win2000-PC erfolgen. Auch Win 9x ist als Plattform möglich aber aufgrund der geringeren Sicherheit des Betriebssystems nicht empfehlenswert.

Die Hardwarevoraussetzungen entsprechen denen von WinNT4.0.

3 Firebox Grundlagen

Die Firebox hat keine eigene Festplatte. Sie hält ihre Daten auf einer kleinen 8 MB RAM Flashdisk. Es ist ein extrem eingeschränktes, an die verwendete Hardware optimal angepasstes Linux-Betriebssystem (Kernel 2.033) implementiert.

Die Firebox verfügt über keine eigene Grafikkarte, Maus- oder Tastaturanschlüsse, daher finden alle Änderungen der Konfiguration mit Hilfe des Policy Managers an der Management Workstation statt.

3.1 Firebox-Voreinstellungen

Zur erstmaligen Verbindung mit der Firebox mit Hilfe des Setup-Wizards muss diese kurzgeschlossen werden (siehe Abschnitt 1.3). Als Standard-Passwort wird „wg“ eingegeben.

3.2 Kommunikation mit der Firebox

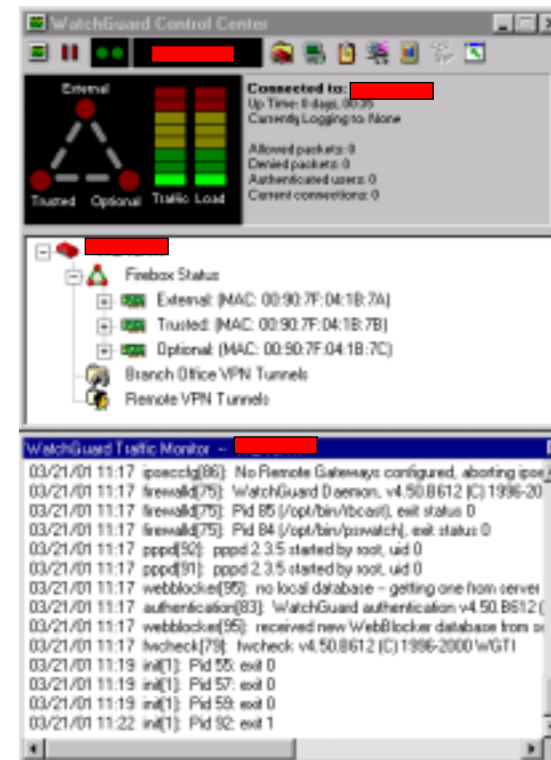
Die Kommunikation mit der Firebox erfolgt über das Control-Center und die darin enthaltenen Tools. Zum Aufbau einer Kommunikation muss daher die Live Security Software installiert werden. Verbindungen können dann über das Netzwerk, ein beiliegendes seriellles Kabel (blau), oder auch via Modem/Pcmcia-Karte aufgebaut werden. Dazu müssen allerdings beide Kennwörter (read-only, und read/write) bekannt sein. Eine zusätzliche Authentifizierung durch ein Java-Applet kann erzwungen werden.

Beim Aufbau der Verbindung sollte zunächst unbedingt nur das read-only Kennwort verwendet werden!

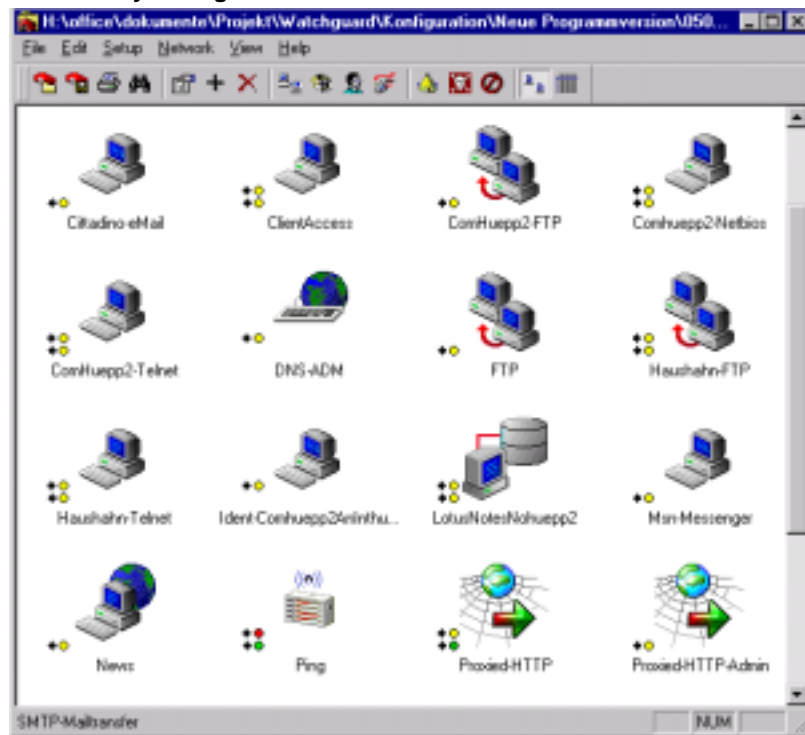
Aus den Policy Manager heraus werden die Konfigurationsdateien und auch das Betriebssystem auf die Firebox übertragen.

3.3 Die LiveSecuritySoftware

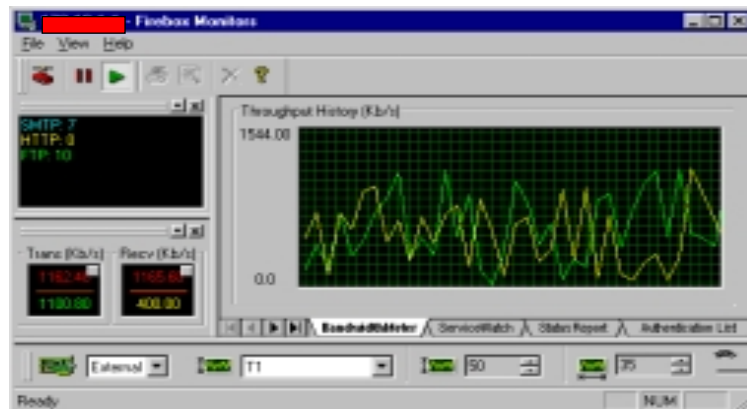
3.3.1 Control Center



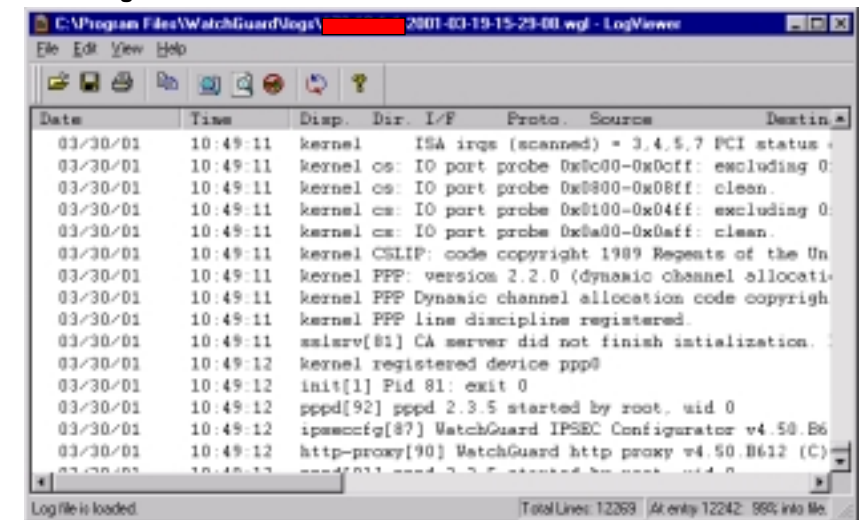
3.3.2 Policy Manager



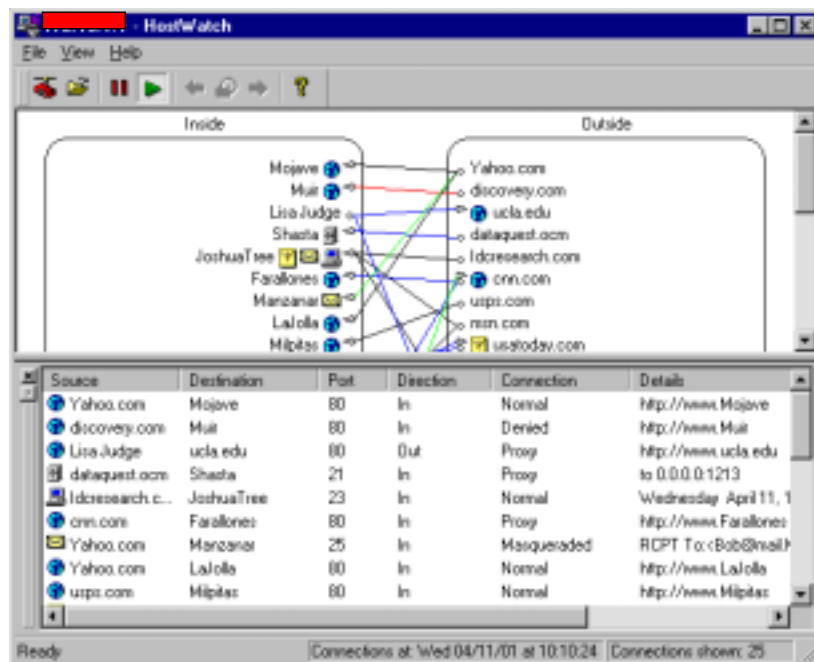
3.3.3 Firebox Monitor



3.3.4 LogViewer

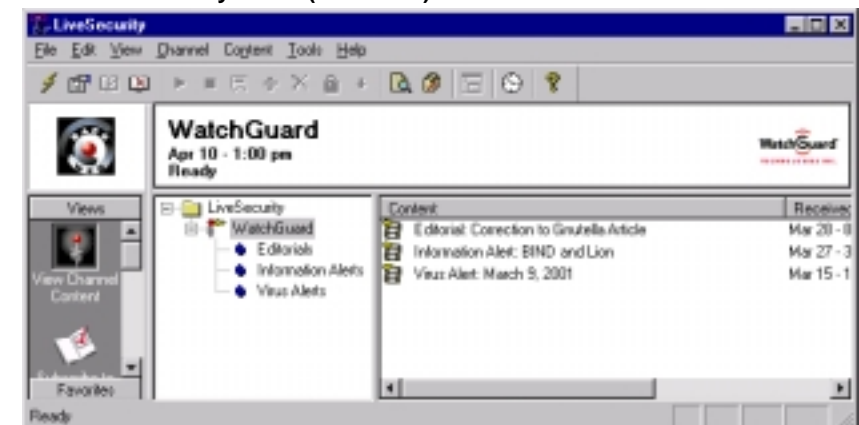


3.3.5 HostWatch



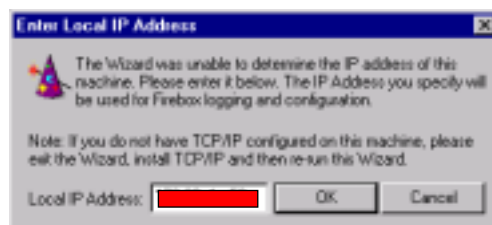
3.3.6 Historical Reports

3.3.7 LiveSecurity Inbox (BackWeb)



4 SetupWizard

Mit Hilfe des Setup-Wizards verbindet man sich das erste Mal mit der Firebox. Dies gilt auch für den Fall, dass die Box aus irgendeinem Grunde nicht mehr erreichbar ist (siehe Notfallplan). Alle notwendigen Informationen zur Verwendung des Setup-Wizards finden sich im InstallGuide. Zur Konfiguration der Hüppe-Firebox wurden im Setup-Wizard die aus den abgebildeten Screenshots ersichtlichen Einstellungen vorgenommen:



WatchGuard QuickSetup Wizard

Firebox CONFIGURATION

Configure Public Servers

Enter the IP address(es) for your public servers. If you do not have any public servers, leave the check boxes empty.

☐ I have an SMTP server behind my Firebox:

☐ I have an HTTP server on the optional interface:

☐ I have an FTP server on the optional interface:

Click the "Next" button to continue.

< Zurück Weiter > Abbrechen Hilfe

WatchGuard QuickSetup Wizard

Firebox CONFIGURATION

Create Firebox Access Passwords

The 'Status' password is used for establishing read-only connections to your Firebox (logging, status, etc.).

Status Password:

Confirm:

The 'Configuration' password is used for establishing read/write connections to your Firebox.

Configuration Password:

Confirm:

Click the "Next" button to continue.

< Zurück Weiter > Abbrechen Hilfe

WatchGuard QuickSetup Wizard

Firebox CONFIGURATION

Upload Security Policy

Choose the Firebox configuration access method:

Use TCP/IP to Configure (Recommended)

The Wizard will communicate and configure your Firebox using Hands-Free Installation technology.

In order to send this security policy to your Firebox, you need to assign it a temporary IP Address so that this machine can communicate with it. This does not have to be the same address that the Firebox's policy is assigned.

Temporary IP Address:

Click the "Next" button and turn on the power to your Firebox.

< Zurück Weiter > Abbrechen Hilfe

Enter Pass Phrase

Enter the current configuration pass phrase for your Firebox. If this is a new installation, use the default below which is set to 'wg'.

Current Configuration Pass Phrase:

OK Cancel

Configuring Firebox

Status: Turn on your firebox now. Waiting...

Cancel

5 Einstellungen

5.1 Ip-Adressen

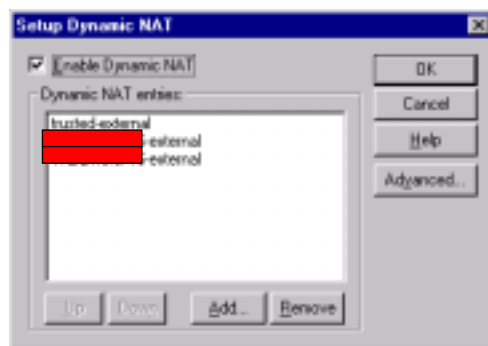
WatchGuard: OBB hat Standard-Einstellungen:

Trusted Interface: xxx.xxx.xxx.xxx
 Optional Interface: xxx.xxx.xxx.xxx
 External Interface: xxx.xxx.xxx.xxx
 Gateway: xxx.xxx.xxx.xxx
 DNS primary: xxx.xxx.xxx.xxx
 DNS secondary: xxx.xxx.xxx.xxx
 WINS-Server: xxx.xxx.xxx.xxx
 Name: WatchGuard
 ManagementStation: xxx.xxx.xxx.xxx
 Loghost: xxx.xxx.xxx.xxx

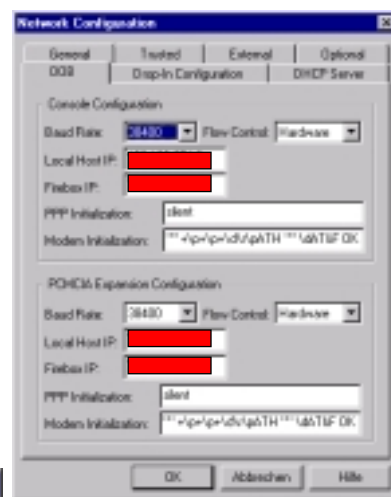
Eingetragene Routes:

xxx.xxx.xxx.xxx/xx -> xxx.xxx.xxx.xxx
 xxx.xxx.xxx.xxx/xx -> xxx.xxx.xxx.xxx
 xxx.xxx.xxx.xxx/xx -> xxx.xxx.xxx.xxx

NAT:



Logging: Live Security Event Processors: xxx.xxx.xxx.xxx



5.2 Authentifizierung

Zur Authentifizierung kann der DHCP01 herangezogen werden. Das heißt, die WatchGuard gibt bei einer Anmeldung die Anfrage nach dem zu authentifizierenden User und dessen Passwort an diesen PDC weiter.

Folgende Aliase sind eingerichtet:

Nr.	Bezeichnung	IP-Adressen
1	external	xxx.xxx.xxx.xxx
2	firebox	
3	trusted	xxx.xxx.xxx.xxx
4	optional	xxx.xxx.xxx.xxx
5	ADM-Einwahl-Adressen	xxx.xxx.xxx.xxx
6	AS/400-Geiger	xxx.xxx.xxx.xxx
7	AS/400-Geiger	xxx.xxx.xxx.xxx
8	As/400-NL	xxx.xxx.xxx.xxx
9	AS/400-NL	xxx.xxx.xxx.xxx
10	Benutzer-NL	xxx.xxx.xxx.xxx/xx
11		xxx.xxx.xxx.xxx
12	Citrix-Server	xxx.xxx.xxx.xxx
		xxx.xxx.xxx.xxx
13	Comhuepp2	xxx.xxx.xxx.xxx
14	Einwahl-Router	xxx.xxx.xxx.xxx
15	Faxhuepp1	xxx.xxx.xxx.xxx
16	Fshuepp3	xxx.xxx.xxx.xxx
17	Geiger	xxx.xxx.xxx.xxx/xx
18	Haushahn	xxx.xxx.xxx.xxx/xx
19	Holland-Router	xxx.xxx.xxx.xxx
20		xxx.xxx.xxx.xxx
21		xxx.xxx.xxx.xxx
22	Hueppe-Admins	xxx.xxx.xxx.xxx
23		xxx.xxx.xxx.xxx
24		xxx.xxx.xxx.xxx
25	Internet-Router	xxx.xxx.xxx.xxx
26	Inthuepp1	xxx.xxx.xxx.xxx
27		xxx.xxx.xxx.xxx
28	LAN-BadZwischenahn	xxx.xxx.xxx.xxx/xx
29	Mailhueppede	xxx.xxx.xxx.xxx
30	Nohuepp2	xxx.xxx.xxx.xxx
31	Pcoak	xxx.xxx.xxx.xxx
32	Pcvsw	xxx.xxx.xxx.xxx
33	Popnw	xxx.xxx.xxx.xxx
34		xxx.xxx.xxx.xxx
35	RS6000	xxx.xxx.xxx.xxx

Zur Anmeldung ruft ein Benutzer in seinem Browser die Adresse: `http://xxx.xxx.xxx.xxx:4100` bzw. `http://xxx.xxx.xxx.xxx:4100` auf. Es wird ihm dann Java-Applet übermittelt, indem er Benutzernamen und Passwort angeben muss. Achtung: Es muss auf Gross- und Kleinschreibung geachtet werden.

Diese Form der Authentifizierung ist auch soweit eingerichtet, wird aber zurzeit noch nicht genutzt.

Bisher sind alle Regeln an die IP-Adresse eines Rechners gebunden. Zur Vereinfachung sind eine Reihe von Aliassen eingerichtet, die in den einzelnen Regeln an Stelle der einzelnen IP-Adressen hinterlegt sind. Dadurch wird zum Einen die Administration übersichtlicher, zum Anderen aber auch einfach, da eine veränderte IP-Adresse lediglich in einem Alias geändert werden muss.

5.3 Paketfilter und Proxies

Aus dem Policy-Manger heraus kann eine Zusammenfassung aller eingestellter Paketfilter und Proxy-Dienste ausgedruckt werden. Die folgende Tabelle zeigt die aktuelle Konfiguration.

Nr.	Filtername	Incoming			Outgoing			Protokoll	QuellPort	Zielpport
		Wert	From	To	Wert	From	To			
1	AnyNL	Allowed	Benutzer-NL Holland-Router	xxx.xxx.xxx.xxx/xx	Allowed	xxx.xxx.xxx.xxx/xx	Benutzer-NL Holland-Router	any	any	any
2	AS/400-Telnet	Allowed	Benutzer-NL	AS/400-NL	Allowed	AS/400-NL	Benutzer-NL	tcp	>1024	23
3	BackWeb-Filter	Denied	None	None	Allowed	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	udp	<1024	370 371
4	Citrix	Denied	None	None	Allowed	xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx	Citrix-Server	tcp	>1024	1494
5	ComHuepp2-Telnet	Allowed	Comhuepp2	pcvsw	Allowed	pcvsw	Comhuepp2	tcp	>1024	23
6	DNS-ADM	Allowed	ADM-Einwahl-Adressen Comhuepp2	Portforward von xxx.xxx.xxx.xxx zu xxx.xxx.xxx.xxx Inthuepp1	Disabled			tcp udp	any	53
7	FTP	Disabled			Allowed	HueppeAdmins	any	ftp	>1024	21
8	Haushahn-FTP	Allowed	Haushahn	RS6000	Allowed	RS6000	Haushahn	ftp	>1024	21
9	Haushahn-Telnet	Allowed	Haushahn	RS6000	Allowed	RS6000	Haushahn	tcp	>1024	23
10	Cittadino-eMail-Wartung	Disabled			Allowed	HueppeAdmins	any	tcp	>1024	8383
11	ClientAccess	Allowed	Geiger	AS/400-Geiger	Allowed	Geiger	AS/400-Geiger	tcp	>1024	23
12	Comhuepp2-Ftp	Disabled			Allowed	pcvsw	Comhuepp2	ftp	>1025	21
13	Comhuepp2-Netbios	Allowed	Comhuepp2	fshuepp3 pcvsw	Allowed	pcvsw fshuepp3	Comhuepp3	udp udp tcp	>1024 >1024 >1024	137 138 139
14	Ident-Comhuepp2An-Inthuepp1	Allowed	Comhuepp2	Portforward von xxx.xxx.xxx.xxx zu xxx.xxx.xxx.xxx Inthuepp1	Disabled			tcp udp	any	113 113

Nr.	Filtername	Incoming			Outgoing			Protokoll	QuellPort	Zielpport
		Wert	From	To	Wert	From	To			
15	LotusNotes-Nohuepp2	Allowed	xxx.xxx.xxx.xxx/xx ADM-Einwahl-Adressen Benutzer-NL	Nohuepp2	Allowed	Nohuepp2	xxx.xxx.xxx.xxx/xx ADM-Einwahl-Adressen Benutzer-NL	tcp	>1024	1352
16	MSN-Messenger	Disabled			Allowed	pcoak	any	tcp	>1024	1080
17	News	Disabled			Allowed	HueppeAdmins	any	tcp	>1024	119
18	Ping	Denied	None	None	Allowed	any	any	icmp	>1024	any
19	Proxied-http	Allowed	Benutzer-NL	any	Allowed	any	any	http udp	>1024	80
20	Proxied-http-Admins	Disabled			Allowed	HueppeAdmins	any	http udp	>1024	80
21	Router-Syslog	Allowed	Comhuepp2 Internet-Router Einwahl-Router Holland-Router	pcoak pcvsw Portforward von xxx.xxx.xxx.xxx zu xxx.xxx.xxx.xxx	Disabled			tcp udp	any	514
22	Router-Wartung	Allowed	Internet-Router Einwahl-Router Holland-Router	pcoak pcosw	Allowed	pcoak pcosw	Internet-Router Einwahl-Router Holland-Router	tcp	>1024	23
23	RouterNL-Port2107	Allowed	Holland-Router	Portforward von xxx.xxx.xxx.xxx zu xxx.xxx.xxx.xxx	Disabled			udp	>1024	2107
24	SMTP-Mailtransfer	Allowed	Comhuepp2 popnw	Portforward von xxx.xxx.xxx.xxx zu xxx.xxx.xxx.xxx	Allowed	Inthuepp1	Comhuepp2 popnw	smtp	any	25
25	WatchGuard	Denied	None	None	Allowed	trused	any	tcp	>1024	4105 4103
26	wg-authentication	Automatisch generiert								

5.4 Logging

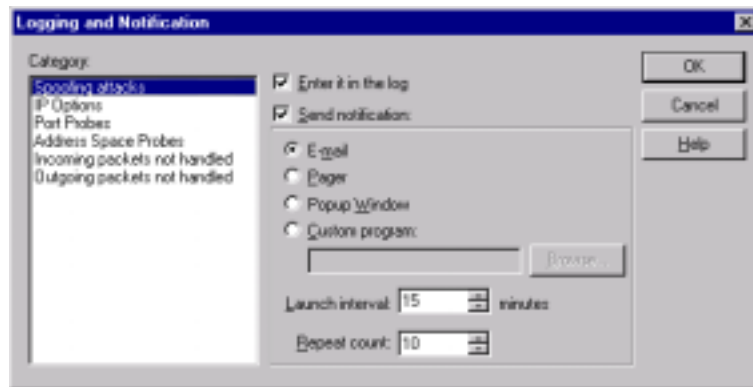
Zum Protokollieren aller Logging-Einträge werden ein oder mehrere Rechner bestimmt. Diese werden im Policy-Manager eingetragen. In unserem Fall ist der PcWatch (xxx.xxx.xxx.xxx) als Logging-Host angegeben.

Darüber hinaus können auch eMails, PopUp-Nachrichten oder Pager-Benachrichtigungen versandt werden.

Im Log-Script werden grundsätzlich alle verdächtigen Pakete (Spoofing, Port-Probes, IP-Options, Address-Space-Probes, Incoming und Outgoing-Pakete, die keiner Regel entsprechen) protokolliert. Für die ersten vier Events wird zusätzlich eine eMail-Benachrichtigung verschickt.

Entsprechende Einstellungen können im Policy Manager vorgenommen werden:

“Setup” – “Default Packet Handling” – “Logging”



Solche Logging-Regeln können für jede einzelne Filterregel bestimmt werden. Diese sind allerdings vor allem für Fehlersuche interessant. Daher wurden die Filter so eingestellt, dass lediglich alle „deny“-Events im Log-Script protokolliert werden.

5.5 Passwörter

Für die Konfigurationsdatei:

Read-only Passwort: xxxxxx

Read-write Passwort: xxxxxx

Live Security Event Processor Encryption Key: xxxxxx

Siehe “Worte.txt” auf der Sicherungsdiskette.

6 Wartung

Konfigurationsänderungen:

Die Konfigurationsdateien sind nach dem Schema: TagMonatJahr.cfg benannt. Bei jeder Konfigurationsänderung sollte diese als neue Konfigurationsdatei abgespeichert werden. Dadurch erhält man eine Art nachvollziehbare Chronologie aller Änderungen und kann jederzeit zu einer älteren, funktionierenden Konfiguration zurückkehren.

Die *.cfg Dateien werden immer automatisch auch auf der Festplatte des administrierenden PCs gespeichert. Sie sollten allerdings bei größeren Änderungen unbedingt zusätzlich auf einer sicher verwahrten Diskette abgelegt werden.

Software-Updates:

In Abständen von etwa einem halben Jahr sendet WatchGuard über einen gesicherten Kanal Software-Updates. Diese enthalten Bugfixes, aber auch zusätzliche Features. Die Updates bauen teilweise aufeinander auf und sollten daher regelmäßig installiert werden. Software-Updates werden zwar auf der Management-Workstation installiert, betreffen jedoch nicht nur die Konfigurations-Software. Bei jeder vollständigen Übertragung einer Policy wird auch das komplette Betriebssystem auf die Firebox übertragen. Die Software-Updates enthalten auch Bugfixes für das Betriebssystem, die auf diesem Wege auf die WatchGuard übertragen werden.

Die Updates kommen immer als *.exe Datei zusammen mit einer Readme.html. Sie werden einfach auf der Management-Workstation installiert. Beim späteren Öffnen der Konfiguration aus der Firebox wird diese nach einer Abfrage in das neue Format konvertiert. Dabei wird im selben Verzeichnis die ursprüngliche Version dieser Datei mit der Erweiterung: *.old abgelegt.

7 Notfallplan

Es sollte nicht passieren, aber es kann passieren. Aus irgendeinem Grund ist die Firebox nicht mehr erreichbar, möglicherweise hat jemand an der Konfiguration herumgespielt oder es hat einen Einbruch gegeben und nun ist man sich nicht sicher, ob auch nichts verändert wurde.

In einem solchen Fall können die folgenden Erklärungen vielleicht erste Hilfestellungen geben.

7.1 Sicherungsdiskette

Wenn die Firewall planmäßig gewartet wurde, ist im Safe eine Sicherungsdiskette vorhanden. Auf dieser sollte sich eine aktuelle Konfigurations-Datei befinden, die aus dem Policy Manager eingespielt werden.

Dazu steckt man die Diskette in das Laufwerk der Management-Workstation, öffnet das WatchGuard Control Center und nach Eingabe des read-only Passwortes den Policy Manager. Dort kann im Menü „File“ der Befehl „open“ – „Open Configuration File“ ausgewählt werden. In dem folgenden Datei Öffnen Dialog sucht man sich die *.cfg-Datei von der Diskette. Um die geöffnete Konfiguration auf die Firebox zu übertragen, wählt man aus dem Menü „File“ den Befehl „Save“ – „to Firebox“. Vor dem Speichern auf der Firebox wird das read/write Kennwort abgefragt.

7.2 Fall: Fehlerhafte Konfiguration

Falls eine fehlerhafte Konfiguration nicht mehr korrigiert werden kann, sollte eine zuvor gesicherte Konfigurationsdatei neu eingespielt werden. Siehe dazu Abschnitt 7.1 .

7.3 Fall: Passwort vergessen

Die Passwörter finden sich in der Datei „Worte.txt“ auf der Sicherungsdiskette. Wenn diese nicht aktualisiert wurden und die Kennwörter auch sonst nicht hinterlegt wurden, kann die Firebox in ihren Lieferungszustand zurückgesetzt (siehe dazu Abschnitt 1.3) werden. Die Konfigurationsdatei muss dann anschließend neu übertragen werden.

7.4 Fall: Update fehlgeschlagen

Das Update betrifft zunächst nur die Management Workstation. Auf dieser muss nach einem fehlgeschlagenen Update die Software neu installiert werden. Von der Konfigurationsdatei wird vor der Übertragung in das neue Format eine Sicherungskopie mit der Erweiterung *.old angelegt. Diese kann in einem solchen Fall zur Rekonstruktion des früheren Standes genutzt werden.

Wenn es sich um richtiges Update der Software auf einer neuen Version handelt, kann diese ohne die Vorgänger-Version installiert werden.

7.5 Fall: Firebox nicht mehr erreichbar

Sollte die Firebox über das Netzwerk nicht mehr erreichbar sein, kann dies mehrere Ursachen haben:

- Die bei der Connectierung eingetragene IP-Adresse der Box stimmt nicht mit der dort eingestellten überein.
- Das Passwort ist nicht richtig.
- Das Routing zwischen der Box und der Workstation funktioniert nicht.
- ...

Entsprechend sollten diese Dinge überprüft werden.

Sonst hat man zwei Möglichkeiten:

- Man versucht die Verbindung mit Hilfe des seriellen Kabels herzustellen (siehe InstallGuide; Seite 12).
- Die Firebox in den Auslieferungszustand zurücksetzen und die Konfigurations-Datei neu übertragen (siehe Abschnitt 1.3).

J. Nessus Scan Report

Number of hosts which were alive during the test : 1

Number of security holes found : 1

Number of security warnings found : 18

Number of security notes found : 8

List of the tested hosts :

192.168.1.200 (Security holes found)

192.168.1.200 :

List of open ports :

- o *ssh (22/tcp) (Security notes found)*
- o *telnet (23/tcp) (Security warnings found)*
- o *time (37/tcp)*
- o *domain (53/tcp) (Security warnings found)*
- o *http (80/tcp) (Security notes found)*
- o *pop3 (110/tcp) (Security notes found)*
- o *sunrpc (111/tcp)*
- o *nnntp (119/tcp) (Security notes found)*
- o *netbios-ssn (139/tcp)*
- o *imap (143/tcp)*
- o *https (443/tcp) (Security warnings found)*
- o *login (513/tcp) (Security warnings found)*
- o *afpovertcp (548/tcp)*
- o *unknown (773/tcp)*
- o *imaps (993/tcp)*
- o *pop3s (995/tcp)*
- o *unknown (1241/tcp)*
- o *unknown (3001/tcp) (Security warnings found)*
- o *squid (3128/tcp) (Security warnings found)*
- o *netbios-ns (137/udp) (Security warnings found)*
- o *general/udp (Security notes found)*
- o *nfs (2049/tcp) (Security hole found)*
- o *unknown (955/udp) (Security warnings found)*
- o *unknown (32768/udp) (Security warnings found)*
- o *unknown (923/udp) (Security warnings found)*
- o *unknown (32772/udp) (Security warnings found)*
- o *nfs (2049/udp) (Security warnings found)*
- o *unknown (770/udp) (Security warnings found)*

Information found on port ssh (22/tcp)

Remote SSH version : ssh-1.99-openssh_2.5.2p2

Warning found on port telnet (23/tcp)

The Telnet service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead.
(<http://www.openssh.com>)

Solution : Comment out the 'telnet' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0619

Information found on port telnet (23/tcp)

Remote telnet banner :

Red Hat Linux release 7.1 (Seawolf)

Kernel 2.4.2-2 on an i686

login:

.....

K. Glossar

Application Level Gateway

Applicationlevel-Gateways arbeiten auf der Anwendungsebene. Während der Paketfilter Pakete, die er für gut befunden hat, passieren lässt, lässt ein Applicationlevel-Gateway nie eine durchgehende Verbindung zu. Er prüft die eingehende Verbindung, kann den Datenstrom analysieren und eröffnet eine neue Verbindung zum Zielgerät im internen Netz. Die Anwendungsdaten, die aus dem Internet empfangen werden, werden durch die Programme des Applicationlevel-Gateways geprüft und eventuell gefiltert an diese neue Verbindung übergeben. Applicationlevel-Gateways gelten als besonders sicher, sind aber nicht so einfach auf neuartige Anwendungen anzupassen.

CERT

Abkürzung für »Computer Emergency Response Team«. Ein Verband, der einen 24-Stunden-Beratungsservice für Internetbenutzer anbietet. CERT kümmert sich dabei um Aspekte, die die Datensicherheit betreffen, und gibt den Benutzern Hilfestellung, wenn neue Viren oder andere Sicherheitslücken entdeckt werden. Die Website des CERT ist unter der Adresse <http://www.cert.org> erreichbar.

[MS Seite 143]

Denial of Service Angriff

(Dienstverweigerungsattacke)

Eine DoS-Attacke übersättigt einen Internetserver mit Verbindungsanforderungen, die nicht ausgeführt werden können. Der Server ist dann mit der Reaktion auf die Attacke so belastet, dass er legitime Verbindungsanforderungen ignoriert.

Bei einem Typ dieser Attacken, unter dem Namen »SYN Flood« bekannt, werden die Zugangsverbindungen des Servers mit falschen Nachrichten überschwemmt.

[MS Seite 200]

DDoS (Distributed Denial of Service)

Eine Form des DoS-Angriffes, die von mehreren Computern ausgeht.

Eine verteilte Dienstverweigerungsattacke besteht darin, in mehrere Computer einzubrechen, dort Programme zu platzieren und sie solange ruhen zu lassen, bis ein Signal gesendet wird, die Attacke vorzunehmen. Ab diesem Zeitpunkt senden all diese Computer einen stetigen Strom von Datenpaketen an die zu attackierende Website und überfordern so die Fähigkeit des Webserver, darauf zu antworten. Da die Attacke von mehreren Computern ausgeht, ist es den Sicherheitseinrichtungen, die sich sonst einer Attacke von nur einem Computer durch Stopp des Datenstromes erwehren können, nicht möglich, die Verbindung zu allen attackierenden Rechnern zu unterbrechen.

Quelle MS Seite 747

Durch solche DoS-Angriffe wurden Anfang 2000 mehrere große Web-Sites wie Amazon.com, Yahoo! und CNN für mehrere Stunden außer Betrieb gesetzt; vgl. SYN message, smurf and fraggle attack, Stacheldraht.

[<http://www.it-infinity.net/servicesupport/d.html>]

DMZ

Demilitarisierte Zone; Ein geschütztes Netzwerk, das zusätzlich zum lokalen Netzwerk (aber getrennt von diesem) für von außen (aus dem Internet) erreichbare Server eingerichtet wird. Hier werden zum Beispiel Web-Server und Mail-Relays eingebunden.

Firewall

Ein »Rechner«, der einem lokalen Netzwerk vorgeschaltet ist. Er dient als Sicherheitssystem, das helfen soll, ein geschlossenes Netzwerk vor Hackern und anderen nicht autorisierten Nutzern zu schützen. Das ganze System beruht meistens auf Kombinationen von Verschlüsselungen, Zugriffsrechten und Kennwörtern und wird sowohl durch die Soft- als auch die Hardware realisiert. [<http://www.it-infinity.net/servicesupport/f.html>]

Hacker

Als Hacker/Cracker bezeichnet man Personen, die sich illegal „.... Zugang zu fremden Computersystemen verschaffen und dann dort Daten ausspionieren oder im teilweise schlimmeren Fall diese Daten unbemerkt manipulieren. (...) Dieses Eindringen erfolgt entweder über offene Zugänge wie Telnet oder rlogin, bei denen die Hacker nur einen Benutzernamen und ein Passwort kennen oder erraten muss, oder über Fehler in anderen Netzwerkdiensten.“ [Strobel, Stefan: Firewalls S. 3]

Als Hacker werden jedoch auch rechtschaffene Programmierer bezeichnet.

Handshaking

Händeschütteln; Austausch von Signalen, der die Kommunikation zwischen zwei Geräten einleitet bzw. ermöglicht und dessen Zweck es ist, die beiden Geräte zu synchronisieren. [<http://www.it-infinity.net/servicesupport/h.html>]

HTTP-Tunnel

In letzter Zeit verbreiten sich zunehmend Programme, die beliebige Daten mit einem bestimmte Format (hier HTML) cachieren und sie so unbemerkt durch eine Firewall zu transferieren, die den offiziellen Transport dieser Daten nicht gestattet hätte. Mit einem solchen Programm ist es zum Beispiel möglich mit einem E-Mail-Client E-Mails aus einem lokalen Netzwerk zu verschicken, obwohl die vorgeschaltete Firewall dafür notwendigen Ports (SMTP:25 und POP3:110) sperrt.

IDS

Intrusion Detection = Angriffserkennung. Es handelt sich um ein Programm, dass den Datenverkehr in einem Netzwerk überwacht und durch Mustervergleich auf bekannte Angriffstechniken prüft. Entdeckte Angriffe werden von diesem Programm gemeldet, sodass sofort etwas dagegen unternommen werden kann und erfolgte Angriffe möglichst nicht unbemerkt bleiben.

IP-spoofing

Schwindeln, Hereinlegen, Austricksen über IP;

Eine Hacker-Methode (Hacker), um unerwünscht in fremde Systeme einzudringen. Bei dieser Methode wird der Ziel-Host mittels eines modifizierten Verbindungsprotokolls hereingelegt, sodass er "glaubt", der Eindringling sei jemand Berechtigter. [<http://www.it-infinity.net/servicesupport/i.html>] Hierzu wird die Quell-IP-Adresse der Datenpakete gefälscht.

Paketfilter

Paketfilter arbeiten auf der Netzwerk- und Paketebene. Sie können daher bestimmte Pakete aufgrund von IP-Adresse, Protokolltyp und Portnummer filtern. Stateful Paketfilter haben zusätzlich Information über den Status von Verbindungen, was eine wesentlich intelligentere Filterung von Paketen gestattet.

Packet Sniffer

Zu Deutsch: »Datenpaketschnüffler«. Ein Gerät und/oder ein Programm, das jedes über ein Netzwerk versendete Datenpaket untersucht. Der Packet Sniffer muss dabei innerhalb des Netzwerksegments installiert werden, das untersucht werden soll. Packet Sniffer wurden entwickelt, um die Beseitigung von Problemen zu erleichtern, die die Netzwerkleistung reduzieren. Inzwischen sind Packet Sniffer allerdings auf einigen Netzwerken zum Sicherheitsrisiko geworden, da sie von Crackern eingesetzt werden können, um unverschlüsselte Daten auszuspähen, z. B. Benutzeridentifikationsnummern, Passwörter, Kreditkartennummern, E-Mail-Adressen und andere vertrauliche Daten. [MS Seite 527]

Ping of Death

Eine Form des Internetvandalismus. Es wird dabei ein Paket gesendet, das wesentlich umfangreicher als die normalen 64 Byte ist. Dieses Paket wird über das Internet mit dem Ping-Protokoll an einen Ferncomputer gesendet. Durch die immense Größe des Pakets stürzt der Empfängercomputer entweder ab oder führt einen Rebootvorgang durch. [MS Seite 547]

POP (Post Office Protocol):

Protokoll für die Übertragung von Mails von einem Server (Post Office) an einen Mail-Client.

Port-Forwarding

Beim Port-Forwarding werden Datenpakete, die an einen bestimmten Zielport gerichtet sind, an eine bestimmte IP-Adresse weitergeleitet. Dadurch wird es beispielsweise möglich einen E-Mail- oder Web-Server mit einer privaten IP-Adresse zu betreiben und sie dennoch aus dem Internet erreichbar zu machen.

Proxy

Ein Server-Dienst, der stellvertretend für die internen Clients mit den externen Servern kommuniziert. Er verhindert eine direkte Verbindung zwischen Quelle und Ziel und ist in der Lage die passierenden Daten auf Anwendungsebene zu untersuchen. Ein Caching Proxy speichert die für die Clients geholten Webseiten.

Das Angebot eines Proxy-Servers dient auch als eine Art Zwischenspeicher für oft abgefragte Seiten des Internets, und der Zugriff des Users erfolgt in der Regel schneller als bei direktem Zugriff.

[<http://www.it-infinity.net/servicesupport/p.html>]

RFC (Request For Comments):

Sammlung von Standards, Vorschlägen für Standards und sonstige Texte, die das Internet betreffen.

Screened-Subnet:

Teilnetz zwischen einem zu schützenden Netz und einem unsicheren Netz, in dem Firewall-Komponenten für die Kontrolle der Verbindungen und Pakete sorgen.

Smurf and fraggle attack

Schlumpf- und Fraggel-Angriff;

DoS attack, bei der ein manipuliertes PING an einen Server geschickt wird, das sich zum einen innerhalb des lokalen Netzwerkes selbst vervielfältigen (broadcast) kann, zum anderen mittels IP-spoofing als Absenderadresse, an die die PING-Antwort geschickt werden soll, die Zieladresse des Servers selbst enthält. Als Ergebnis bricht der angegriffene Server unter der Last der eigenen PING-Antworten zusammen.

[<http://www.it-infinity.net/servicesupport/s.html>]

Spam-Relay

Ein Server, der zum Versand von sogenannten Spam-Mails missbraucht wird. Das heißt über diesen Server können beliebig viele unerwünschte E-Mails an Dritte verschickt werden. Häufig fordern solche Mail-Server vom Absender einer E-Mail keine Authentisierung an. Infolgedessen können E-Mails mit beliebigem Absender verschickt werden. Der Absender einer Vireninfiltrierten E-Mail bleibt so unentdeckt.

SYN message

DoS attack, bei der sich jemand die Spezifika von TCP/IP zunutze macht: Eine Eigenschaft von TCP/IP ist es, beim Verbindungsaufbau (handshaking) auf einen PING mit einem ACK zu antworten. Hat das Betriebssystem eines Servers keinen Mechanismus eingebaut, nach einer bestimmten Anzahl von PINGs eine Antwort zu verweigern, bricht der Server unter der Last einer ganzen Flut von PINGs zusammen.

[<http://www.it-infinity.net/servicesupport/s.html>]

Trojan horse

Trojanisches Pferd; Virenprogramm (Virus), das in harmloser "Verkleidung" auftritt, wie z. B. als Packprogramm, Spiel oder sogar als Programm, das Viren finden und zerstören soll (z. B. mockingbird).

[<http://www.it-infinity.net/servicesupport/t.html>]

Solche Programme sind häufig auch in der Lage einem Angreifer die Kontrolle über den befallenen Rechner zu verschaffen.

VPN

Virtuell Private Network. Mit Hilfe des VPNs können IP-Tunnel für die Einwahl von außen erstellt werden. Ähnlich wie bei dem RAS-Dienst (Remote Access) wird eine „direkte“ Verbindung zum lokalen Netzwerk aufgebaut. Allerdings findet die Datenübertragung in einem VPN-Netz verschlüsselt statt. Im Gegensatz zum RAS, der die Einwahl eines Clients über eine Telefonverbindung realisiert verwendet VPN das Internet. Im Vergleich zu Telefonferngesprächen ist die Datenübertragung via Internet meist wesentlich preisgünstig.

Virus

Analogie aus der Medizin: Programm, das auf Computer und/oder Software ähnlich einwirkt wie ein biologischer Virus auf einen lebenden Organismus. Ziel und Zweck eines Computervirus ist es, sich zu verbreiten, d. h. über jede Art des Datenaustausches in andere Computer zu gelangen, sich dort an Programmdateien anzuhängen und diese zu verändern – meistens zum Negativen.

Ein Virus ist ein Programm, das Kopien von sich selbst in Computerdateien einfügt und diese damit »infiziert«. Sobald man eine derartige Datei in den Speicher lädt und startet, wird in der Regel auch eine Kopie des Virus aktiviert, der damit andere Dateien »befallen« kann. Viren haben oft zerstörerische Wirkung auf Datenbestände, die zum Teil beabsichtigt sind. Einige Viren können z. B. die Festplatte eines Computers zerstören oder Speicherplatz einnehmen, der anderenfalls von Programmen verwendet werden könnte. [MS Seite 759]

Wurm

Ein Virenprogramm, das sich in Computersystemen fortpflanzen kann, indem es in den Arbeitsspeichern der betroffenen Systeme Kopien von sich erstellt. Dabei kann sich ein Wurm innerhalb eines Computersystems so oft duplizieren, dass das System abstürzt. Ein Wurm kann auch aus einzelnen, separat programmierten Segmenten bestehen. Er wird unbemerkt in ein Hostsystem eingeschleust, was unter Computerfachleuten manchmal als Scherz verstanden wird, oft aber auch gezielt erfolgt, um Informationen zu zerstören. [MS Seite 784]

IBM Global-Network

IBM bietet mit Global Network ein separates Datennetzwerk für Firmen an. Über dieses Netzwerk kann wahlweise TCP/IP aber auch SNA übertragen werden.