IBM SecureWay FirstSecure

Planung und Integration

Version 2

IBM SecureWay FirstSecure

Planung und Integration

Version 2

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter Anhang A, „Bemerkungen“ auf Seite 103, gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des
IBM SecureWay FirstSecure Planning and Integration,
IBM Form CT7EHNA,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
November 1999

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellen

Zu diesem Handbuch

IBM SecureWay FirstSecure (auch FirstSecure genannt) ist ein benutzerfreundliches Gerüst, mit dem ein Unternehmen

- alle Aspekte des Netzbetriebs über das Web und andere Netze sichern kann.
- auf den bereits vorhandenen Investitionen in e-business aufbauen kann. Durch die modulare Struktur der Angebote kann der Ausbau der Sicherheit je nach Bedarf vorgenommen werden.
- die Gesamtkosten für ein gesichertes e-business reduzieren kann.

In diesem Buch werden FirstSecure und die Produkte beschrieben, aus denen FirstSecure besteht. Zudem enthält es erste Informationen über die Planung der Benutzung dieser Produkte.

Die in diesem Buch beschriebenen Produkte sind Teil einer stufenweisen Freigabe. Möglicherweise sind nicht alle Produkte gleichzeitig oder in allen Ländern verfügbar. Nehmen Sie Kontakt mit dem IBM Vertriebsbeauftragten auf, wenn Sie Informationen über die Verfügbarkeit der einzelnen Produkte benötigen.

Abbildungen in diesem Buch

Die Abbildungen in diesem Buch dienen nur zu Planungszwecken. In den einzelnen Abbildungen ist jeweils nur eine der vielen Anordnungsmöglichkeiten von Servern, Clients und Anwendungen dargestellt, die für Ihr Unternehmen bestehen können.

Das Format der Abbildungen hängt davon ab, in welchem Format das Buch geliefert wird:

- Die meisten Abbildungen in der PDF-Version des Buchs sind einfacher gestaltet, damit Plattenspeicherplatz eingespart wird und die Abbildungen schneller gedruckt werden.
- Abbildungen in der gedruckten Version sind komplexer, belegen mehr Speicherplatz und werden langsamer geruckt.

Die Abbildungen sind in beiden Versionen funktional vergleichbar und haben identische Bildunterschriften und alternativen Text.

Zielgruppe

Dieses Buch ist für Systemadministratoren bestimmt, die für die Planung und Integration der Sicherheit von web-gestützten Systemen zuständig sind. Es sind Kenntnisse des Netzbetriebs und der e-business-Anwendungen erforderlich.

Aufbau des Handbuchs

Dieses Buch besteht aus den folgenden Teilen:

- Teil 1, „Übersicht über FirstSecure“ auf Seite 1, enthält eine Übersicht über FirstSecure, die FirstSecure-Komponenten und die verfügbaren Angebote.
- In Teil 2, „Gesichertes e-business-Netz planen“ auf Seite 17, wird die Planung eines gesicherten e-business-Netzes beschrieben.
- In Teil 3, „Voraussetzungen für die Installation und Integration“ auf Seite 57, werden die Installationsvoraussetzungen und die Integrationsdetails der FirstSecure-Produkte beschrieben.
- In Kapitel 16, „Mit FirstSecure gelieferte Dokumentationen“ auf Seite 91, sind alle für FirstSecure verfügbaren Dokumentationen beschrieben.
- Im „Glossar“ auf Seite 107 sind die die Sicherheit betreffenden Begriffe aufgeführt, die in diesem Buch benutzt werden.

Dieses Buch enthält zudem ein Literaturverzeichnis, in dem die Dokumentationen zu den einzelnen Produkten beschrieben sind.

Jahr 2000

Nachfolgend wird die Jahr-2000-Konformität von IBM SecureWay FirstSecure beschrieben.

IBM Produkte in IBM SecureWay FirstSecure

Diese Produkte sind Jahr-2000-konform, d. h., sie sind bei Benutzung gemäß der dazugehörigen IBM Dokumentation in der Lage, Datumsdaten innerhalb und zwischen dem 20. und dem 21. Jahrhundert korrekt zu verarbeiten, bereitzustellen und/oder zu empfangen, vorausgesetzt, daß alle anderen Produkte (z. B. Hardware, Software, Firmware), die zusammen mit ihnen benutzt werden, präzise Datumsdaten ordnungsgemäß mit ihnen austauschen.

Produkte anderer Lieferanten

Für andere Produkte wurde gegenüber IBM bestätigt, daß diese Produkte Jahr-2000-konform sind. IBM trifft diesbezüglich keine Aussagen und übernimmt keine Gewährleistung für die Jahr-2000-Konformität dieser Produkte. Bei Fragen bezüglich der Jahr-2000-Konformität dieser Produkte wenden Sie sich bitte direkt an den Hersteller. Die Informationen über Produkte und Services anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat den Inhalt dieser Veröffentlichungen nicht gesondert überprüft und übernimmt keine Verantwortung für die Richtigkeit und Vollständigkeit der Informationen in diesen Veröffentlichungen.

Service und Unterstützung

Nehmen Sie Kontakt mit IBM auf, wenn Sie für ein Produkt des SecureWay FirstSecure-Angebots Service und Unterstützung benötigen. In den Dokumentationen für einige dieser Produkte wird auf die Kontaktaufnahme mit anderen Unternehmen hingewiesen, wenn Service und Unterstützung benötigt werden. Werden diese Produkte als Bestandteil des SecureWay FirstSecure-Angebots geliefert, nehmen Sie Kontakt mit IBM auf, wenn Sie Service und Unterstützung benötigen.

Konventionen

In diesem Buch werden die folgenden Konventionen benutzt:

- **Fettdruck**: Namen von auszuwählenden Elementen, Namen von Befehlen, Text, den ein Benutzer eingibt, oder Beispiele im Fließtext sind **fett** dargestellt.
- `Monospace-Schrift`: Beispiele (wie fiktive Pfad- oder Dateinamen) sowie Texte, die in Anzeigen erscheinen, sind in `Monospace-Schrift` dargestellt.

Web-Informationen

Information über die neuesten Aktualisierungen an FirstSecure sind im Internet unter www.ibm.com/software/security an folgenden Stellen zu finden:

IBM SecureWay FirstSecure
www.ibm.com/software/security/firstsecure

Die Dokumentationen sind verfügbar unter
www.ibm.com/software/security/firstsecure/library

IBM SecureWay Policy Director
www.ibm.com/software/security/policy

Die Dokumentationen sind verfügbar unter
www.ibm.com/software/security/policy/library

IBM SecureWay Boundary Server
www.ibm.com/software/boundary

Die Dokumentationen sind verfügbar unter
www.ibm.com/software/boundary/library

IBM SecureWay Trust Authority
www.ibm.com/software/security/trust

Die Dokumentationen sind verfügbar unter
www.ibm.com/software/securitytrust/library

Das ITSO-Redbook *Understanding the IBM SecureWay FirstSecure Framework*, IBM Form SG24-5498-00, ist im Internet unter www.ibm.com/redbooks verfügbar.

Teil 1. Übersicht über FirstSecure

Dieser Teil enthält eine Übersicht über FirstSecure und die FirstSecure-Komponenten. Zudem werden die einzelnen Produkte kurz beschrieben.

In diesem Teil werden auch die IBM Implementierungsservices beschrieben.

Kapitel 1. Beschreibung von FirstSecure

IBM SecureWay FirstSecure ist Teil der integrierten IBM Sicherheitslösungen. FirstSecure ist eine benutzerfreundliche Gruppe von Modulen, mit denen ein Unternehmen

- eine gesicherte e-business-Umgebung einrichten kann.
- die Gesamtkosten für ein gesichertes Netz durch Vereinfachung der Sicherheitsplanung reduzieren kann.
- Sicherheitsrichtlinien leichter implementieren kann.
- eine effektivere e-business-Umgebung erstellen kann.

Die FirstSecure-Komponenten bietet Virenschutz, das Erkennen von Attacken auf das System, Zugriffssteuerung, Steuerung des Datenverkehrsinhalts, Verschlüsselung, digitale Zertifikate, Firewall-Technologie und Anwendungsentwicklungs-Toolkits. Diese Funktionen werden über die IBM SecureWay-Produktfamilie sowie über Angebote anderer Lieferanten zur Verfügung gestellt. Durch die Kombination der jeweils besten Komponenten verschiedener Anbieter von Sicherheitsprodukten wird eine optimale Sicherheitslösung erreicht. Zudem stehen für ausgewählte FirstSecure-Komponenten Implementierungsservices zur Verfügung. FirstSecure besteht aus folgenden Modulen:

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- Public Key Infrastructure, verfügbar über IBM SecureWay Trust Authority
- IBM SecureWay Toolbox

Da FirstSecure aus einer Gruppe von Produkten besteht, die unabhängig voneinander installiert werden können, kann der Übergang auf eine gesicherte Umgebung den Anforderungen entsprechend erfolgen. Sie können in einem bestimmten Bereich beginnen, die Verbesserungen testen und dann die Sicherheit kontinuierlich verbessern. Auf diese Weise werden Komplexität und Kosten verringert, und Web-Anwendungen und -Ressourcen können schneller genutzt werden.

Vorteile von FirstSecure

Ihre Daten und Ressourcen sind wichtig für Ihr e-business. Gemeinsam bieten die FirstSecure-Produkte folgendes:

Schutz durch Vergabe von Berechtigungen
Jeder muß die Regeln befolgen. Durch die Vergabe von Berechtigungen können nur zugelassene Benutzer auf die Systeme, Daten, Anwendungen und Netze zugreifen.

Schutz durch Überprüfbarkeit
Sie können ermitteln, wer wann welche Aktion vorgenommen hat. Durch die Überprüfbarkeit können Sie ermitteln, wer eine Aktion vorgenommen hat und welche Aktionen innerhalb eines bestimmten Zeitintervalls vorgenommen wurden.

Schutz durch Zuverlässigkeit
Sie können sicher sein, daß das System die versprochene Sicherheit bietet und die geforderte Stufe der Sicherheit erzwungen wird.

Schutz durch Verfügbarkeit
Das System ist verfügbar, wann immer es benötigt wird. Durch diesen Schutz bleiben Systeme, Daten, Netze und Anwendungen für Mitarbeiter, Lieferanten, Geschäftspartner und Kunden verfügbar.

Schutz durch Verwaltbarkeit
Sie können die Regeln definieren. Durch diesen Schutz können Sie Richtlinieninformationen definieren, verwalten, überwachen und ändern.

Sie können diesen Schutz auf der Basis unternehmensweiter Richtlinien implementieren, damit das gesamte Geflecht aus Netzen, Systemen und Anwendungen in Ihrem Unternehmen geschützt ist, da eine einzige Schwachstelle zwischen Produkten in diesem Geflecht die restliche Infrastruktur nutzlos machen könnte.

In diesem Buch wird gezeigt, wie die SecureWay-Module zum Schutz des Geflechts eingebunden werden können.

FirstSecure-Module

FirstSecure enthält Produkte, die Sie als gesamte Gruppe oder als separate Produkte bestellen können. Die einzelnen Produkte können wiederum Komponenten enthalten. Sie können mit einem beliebigen Produkt beginnen und nach und nach eine vollständige Sicherheitslösung aufbauen.

Policy Director

Der Policy Director steht im Mittelpunkt der Sicherheitsplanung. Der Policy Director bietet Berechtigungs- und Verwaltungsfunktionen, die die Endpunkt-zu-Endpunkt-Sicherheit von Web-Ressourcen über geografisch weit verstreute Intranets und Extranets ermöglichen. Der Policy Director bietet Services zur Authentifizierungs-, Berechtigungs-, Datensicherheits- und Ressourcenverwaltung. Der Policy Director wird zusammen mit Internet-gestützten Standardanwendungen benutzt, um gesicherte und gut verwaltete Intranets aufzubauen. Der Policy Director beinhaltet folgendes:

- Sicherheitsservices
- Verwaltungskonsole (Management Console)
- Verwaltungs-Server
- Security Manager (NetSEAL und WebSEAL)
- NetSEAT-Client
- Directory Services Broker
- Berechtigungs-Server (Anwendungsunterstützung eines anderen Anbieters)

Der Policy Director läuft unter Windows NT, AIX und Solaris.

In Kapitel 5, „Policy Director im Netz planen“ auf Seite 33, ist der Policy Director ausführlich beschrieben.

SecureWay Boundary Server

Die SecureWay Boundary Server-Produkte bieten Zuverlässigkeit, Verwaltbarkeit und Überprüfbarkeit für web-gestützte e-business-Anwendungen. Gesicherte Grenzen werden überall benötigt — zwischen Abteilungen wie der technischen Abteilung und der Personalabteilung, zwischen den Netzen der Zentrale und fernen Geschäftsstellen, zwischen dem Netz des Unternehmens und dem Internet, zwischen den Web-Anwendungen des Unternehmens und den Kunden und zwischen dem Netz des Unternehmens und den Geschäftspartnern. Eine ordnungsgemäße Sicherheit von Grenzen setzt voraus, daß gesteuert wird, wer auf Ihr Netz zugreifen kann und welche Informationen in Ihr Netz gelangen und Ihr Netz verlassen können.

In diesem Abschnitt werden die SecureWay Boundary Server-Module beschrieben. Überlegungen zur Planung und Integration enthält Kapitel 12, „SecureWay Boundary Server - Voraussetzungen und Überlegungen zur Installation“ auf Seite 63.

IBM SecureWay Firewall

IBM SecureWay Firewall, auch als IBM Firewall bezeichnet, ermöglicht sichere e-business-Operationen, indem alle Übertragungen in das und aus dem Internet gesteuert werden. IBM Firewall beinhaltet die drei wichtigen Firewall-Architekturen (Filter, Proxy und Circiut-Level-Gateway), damit Kunden ein hohes Maß an Sicherheit und Flexibilität geboten wird.

ACE/Server

Der ACE/Server von Security Dynamic enthält SecurID-Token (2 Benutzerlizenzen und 2 Token). Der ACE/Server fügt IBM SecureWay Firewall eine Administrator-Anmeldung und eine Verbindung für ein *virtuelles privates Netz (VPN)* hinzu.

MIMEsweeper für IBM SecureWay Release 2

MIMEsweeper von Content Technology enthält Komponenten für die Sicherheit im Internet. MAILsweeper überprüft E-Mail, um sicherzustellen, daß keine vertraulichen Informationen Ihr Netz verlassen können und keine unerlaubte E-Mail in Ihr Netz gelangt.

WEBsweeper verhindert, daß unerwünschtes Web-Material in Ihr Netz gelangt. WEBsweeper durchsucht Daten und akzeptiert nur Daten von zulässigen Java-Minianwendungen, ausführbaren Codes oder Web-Sites.

SurfinGate

SurfinGate von Finjan Software Ltd. ist eine Sicherheitslösung zur Überwachung von mobilem Code für das e-business. Da mobiler Code oft automatisch und routinemäßig von außen in Ihr e-business-Netz gelangt, reicht der Schutz durch Firewalls nicht aus. SurfinGate schützt Ihr Netz gegen Attacken durch Java-, ActiveX- und JavaScript-Code. SurfinGate erkennt mögliche feindliche Attacken, bevor sie in das Netz gelangen können und hält sie dadurch von Ihren kritischen Ressourcen fern. SurfinGate isoliert verdächtige Daten, damit sie überprüft werden können, bevor sie akzeptiert werden.

Intrusion Immunity

Intrusion Immunity bietet zuverlässige Sicherheit durch Produkte, die feindliche Attacken erkennen und das System gegen solche Attacken schützen. In Kapitel 13, „Intrusion Immunity - Voraussetzungen und Überlegungen zur Installation“ auf Seite 71, sind die Voraussetzungen für Intrusion Immunity aufgeführt. Intrusion Immunity beinhaltet Tivoli Cross-Site for Security und Norton AntiVirus.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security schützt Systeme, die anfällig für feindliche Attacken sind, durch das Erkennen von Attacken. Mit Tivoli Cross-Site for Security ist folgendes möglich:

- Cross-Site for Security-Agents im Netz installieren, um dem Cross-Site for Security-Verwaltungs-Server verdächtige Ereignisse zu berichten.
- Daten, die eine Attacke auf die Systemsicherheit darstellen, in vordefinierten und angepaßten Berichten überprüfen.
- Unbefugte oder verdächtige Aktivitäten in Echtzeit erkennen und protokollieren.
- Sicherheits-Agents optimieren, um die Anzahl falscher Alarme zu reduzieren.

Norton AntiVirus

Norton AntiVirus, ein Produkt der Symantec Corporation, ist eines der weltweit führenden Antivirusprodukte. Norton AntiVirus kann permanent im Hintergrund laufen und den Computer gegen Viren schützen, die über E-Mail-Anlagen, ActiveX-Steuerungen, Java-Minianwendungen, heruntergeladene Internet-Dateien, Disketten, Software-CDs oder über ein Netz gesendete Dateien eindringen können. Mit Norton AntiVirus können infizierte Dateien isoliert werden. Norton AntiVirus kann so konfiguriert werden, daß Sie automatisch über Aktualisierungen und neu festgestellte Viren informiert werden.

Public Key Infrastructure

IBM FirstSecure unterstützt PKI-Standards (PKI = Public Key Infrastructure) für die Verschlüsselung und die Interoperabilität über das Produkt IBM SecureWay Trust Authority.

SecureWay Trust Authority ist eine Sicherheitslösung, die das Ausgeben, Erneuern und Widerrufen von digitalen Zertifikaten unterstützt. Diese Zertifikate können in einem weiten Bereich von Internet-Anwendungen eingesetzt werden und bieten ein Mittel zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation. Trust Authority basiert auf den Spezifikationen der *Internet Engineering Task Force* (IETF) *Public Key Infrastructure* (PKI) Working Group und beinhaltet folgendes:

- Unterstützung für IBM AIX- und Microsoft Windows NT-Server.
- Eine Registrierungsstelle (RA).
- Eine Zertifizierungsstelle (CA).
- Benutzerschnittstellen zum Anfordern von Zertifikaten und zum Verwalten ausgegebener Zertifikate.
- Eine integriertes *IBM SecureWay Directory*.
- Ein *Protokollierungssubsystem*.
- Unterstützung für den SecureWay PCI 4758 Cryptographic Coprocessor.
- Unterstützung für *Smart Cards*.

Diese Infrastruktur unterstützt die gesamte Lebensdauer von Zertifikaten einschließlich der Registrierung und ersten Zertifizierung, der Aktualisierung von Schlüsselpaaren, der Erneuerung von Zertifikaten, der Veröffentlichung von Listen mit erteilten und widerrufenen Zertifikaten und der Widerrufung von Zertifikaten. Weitere Informationen enthält Kapitel 14, „Public Key Infrastructure - Voraussetzungen und Überlegungen zur Installation“ auf Seite 79.

Toolbox

Die FirstSecure Toolbox ist eine Gruppe von Sicherheits- und sicherheitsbezogenen Toolkits, die Teil der wichtigen FirstSecure-Komponenten sind oder Interoperabilität mit den FirstSecure-Komponenten aufweisen. Die Toolkits sind für folgendes hilfreich:

- Integration der Anwendungen mit FirstSecure.
- Anpassung von Lösungen und Anwendungen mit FirstSecure.
- Erstellung von ISV- und OEM-Anwendungen, die FirstSecure nutzen.

Die FirstSecure Toolbox-Toolkit-APIs unterstützen die folgenden Sicherheitsfunktionen:

- Berechtigungsservices
- Zertifizierungs- und Verwaltungsservices
- Verzeichnisservices
- Secure Sockets Layer-Protokollservices
- KeyWorks-Services für Verschlüsselungs- und Authentifizierungsverwaltung
  - IBM Key Recovery Service Provider 1.1.3.0-APIs. Der IBM Key Recovery Service Provider ermöglicht die Wiederherstellung verschlüsselter Informationen.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 ist eine Anwendung, die nach einer berechtigten Anforderung verschlüsselte Informationen wiederherstellen kann, wenn Schlüssel unverfügbar, verlorengegangen oder beschädigt sind.

    Diese beiden Toolkits bieten Standardschnittstellen, über die Anwendungen kritische Sicherheitsservices aufrufen und Anbieter von Sicherheitsprodukten ihre Produkte in das Toolkit integrieren können. Die Standardschnittstellen basieren auf der CDSA-Architektur (CDSA = Common Data Security Architecture). Diese Toolkits sind unter Windows NT, Solaris und AIX verfügbar.

Implementierungsservices

Mit den FirstSecure-Implementierungsservices ist FirstSecure schnell für Ihr e-business einsatzbereit. Diese kostenpflichtigen separaten Services werden von IBM zur Verfügung gestellt und von einem erfahrenen Team von Beratern ausgeführt. Die FirstSecure-Implementierungsservices beinhalten einen FirstSecure-Implementierungs-Workshop und Installationsservices für einen schnellen Start (QuickStart) auf Produktebene. IBM bietet auch FirstSecure-Systemintegrationsservices an, die an die jeweiligen Umgebungen angepaßt sind.

Nehmen Sie Kontakt mit dem IBM Ansprechpartner auf, wenn Sie Informationen über Produkte und Preise benötigen.

Kapitel 2. Neuerungen in Release 2

Release 2 vereinfacht die Planung und Installation der IBM SecureWay FirstSecure-Produkte. Die einzelnen Produkte können besser integriert werden, es wurden Produkte hinzugefügt, und die Verwaltung und Steuerung kann zentraler erfolgen.

Policy Director

Der Policy Director bietet die folgenden Erweiterungen:

- Unterstützung für das IBM SecureWay Directory zum Speichern von Informationen über die Berechtigung von Benutzern und Gruppen.
- Neueste Aktualisierungen an der Spezifikation der Authorization API der Open Group.
- Fähigkeit zum Definieren und Bearbeiten der Berechtigungen von IBM Firewall-Proxy-Benutzern über die Policy Director-Verwaltungskonsole (Management Console).
- Policy Director Credentials Acquisition Service (CAS), der die Benutzung externer Authentifizierungsservices unterstützt.
- Unterstützung der zertifikatgestützten Authentifizierung auf Client-Seite über den neuen Policy Director Credentials Acquisition Service (CAS).
- Fähigkeit zum Schreiben eigener angepaßter CAS-Funktionen über die IDL-Schnittstelle (IDL = Interface Definition Language) zwischen WebSEAL und dem Policy Director-CAS. Der Policy Director bietet zudem das allgemeine Server-Gerüst, das die Policy Director-CAS-Server-Funktionen verarbeitet, beispielsweise das Starten, die Server-Registrierung und die Signalverarbeitung.
- Möglichkeit zur Benutzung eines SSL-Tunnelmechanismus (SSL = Secure Sockets Layer) zusätzlich zu dem GSS-Tunnelmechanismus (GSS = Generic Security Services).
- Benutzung der Policy Director-Verwaltungskonsole (Management Console) oder -Befehlszeilenschnittstelle zur Verwaltung der Richtlinien für Anmeldung und Kennwort.
- Benutzung der Policy Director-Verwaltungskonsole (Management Console) oder -Befehlszeilenschnittstelle zur Verwaltung von Benutzern, Gruppen und Ressourcen (Ziele) mit einstufiger Anmeldung.
- Web-gestütztes Tool zur Verwaltung der Kennwörter von Zielen (Benutzern, Gruppen und Ressourcen) mit einstufiger Anmeldung.
- Integrierter Installationsprozeß.

SecureWay Boundary Server

Der SecureWay Boundary Server bietet die folgenden Erweiterungen:

- Eine grafische Benutzerschnittstelle für die Konfiguration, die bestimmte Funktionen von SecureWay Boundary Server und Policy Director zusammenfaßt.
- Ein neuer TaskGuide für die Konfiguration, der bestimmte Funktionen von SecureWay Boundary Server und Policy Director zusammenfaßt.

Neuerungen in IBM SecureWay Firewall für AIX und NT

IBM SecureWay Firewall, auch IBM Firewall genannt, bietet die folgenden Erweiterungen:

Erweiterungen am Proxy für gesicherte Post

Der IBM Firewall-Proxy für gesicherte Post wurde erweitert und enthält die folgenden neuen Funktionen:

- Anti-SPAM-Algorithmen, mit denen Nachrichten bekannter Spammer über Ausschlußlisten abgewehrt und Nachrichten auf Gültigkeit und Wiederholbarkeit überprüft werden können (bekannte Wege zum Abwehren unerwünschter Nachrichten) und die Anzahl von Empfängern pro Nachricht und die maximale Größe einer Nachricht begrenzt werden kann.
- Anti-Spoofing-Unterstützung einschließlich der Integration leistungsfähiger Authentifizierungsmechanismen.
- Unterstützung für SNMP-Alarmnachrichten und die MADMAN-MIB.
- Nachrichtenüberwachung einschließlich der Fähigkeit zum nahtlosen Verfolgen von Nachrichten zwischen Firewall und Backend-Post-Server (Domino).

Erweiterungen am Socks-Protokoll Version 5

Das Socks-Protokoll Version 5 wurde durch eine Authentifizierung mit Benutzername und Kennwort, eine Authentifizierung von Anforderung und Antwort und Authentifizierungs-Plug-Ins erweitert.

Die Protokollierung wurde erweitert, damit Benutzer bessere Steuerungsmöglichkeiten bei der Klassifizierung von Protokollnachrichten und bei der Angabe von Protokollstufen haben.

HTTP-Proxy

IBM SecureWay Firewall bietet eine HTTP-Proxy-Implementierung mit allen Funktionen, die auf dem Produkt IBM Web Traffic Express (WTE) basiert. Der HTTP-Proxy bearbeitet Browser-Anforderungen effizient über IBM Firewall, ein Socks-Server ist für die Suche im Internet daher nicht erforderlich. Benutzer können auf nützliche Informationen im Internet zugreifen, ohne daß die Sicherheit ihrer internen Netze gefährdet ist und ihre Client-Umgebung zur Implementierung des HTTP-Proxy geändert werden muß.

RAS-Dienst

Der Windows NT RAS-Dienst (Remote Access Service) bietet Netzanschlüsse über Wählverbindungen, ISDN-Verbindungen oder X.25-Verbindungen mit dem Protokoll für Punkt-zu-Punkt-Verbindungen (Point-to-Point Protocol, PPP). NDISWAN ist ein Treiber für den Netzbetrieb, der als Teil des RAS-Dienstes geliefert wird und die untergelegten PPP-Daten so umsetzt, daß sie Ethernet-LAN-Daten ähnlich sind.

IBM SecureWay Firewall-Erweiterungen für AIX

IBM SecureWay Firewall für AIX bietet zahlreiche Erweiterungen:

Erweiterte IPSec-Unterstützung
: Die erweiterte IPSec-Unterstützung beinhaltet Unterstützung für neue Kopfzeilenbereiche. Zudem werden die Interoperabilität mit mehreren IBM Servern und Routern sowie viele nicht von IBM stammende VPN-Produkte unterstützt, die die neuen Kopfzeilenbereiche unterstützen.

Mehrprozessorunterstützung
: Firewall-Benutzer können die RS/6000-Mehrprozessoreinrichtungen zur Skalierungs- und Leistungsverbesserung nutzen.

Filtererweiterungen
: Die Leistung und Flexibilität bei der Konfiguration wird erhöht. Sie können die Leistung von IBM SecureWay Firewall optimieren, indem Sie die Position unterschiedlicher Arten von Filterregeln auswählen können. Zudem wird protokolliert, wie oft eine Verbindung benutzt wird.

Netzadressenumsetzung
: Die Viele-zu-Eins-Adressenumsetzung wird unterstützt. Bei dieser Zuordnung werden mehrere interne unregistrierte oder private Adressen über Anschlußnummern einer registrierten gültigen Adresse zugeordnet, um die eindeutigen Zuordnungen zu erstellen.

Konfigurationsassistent
: Ein Assistent ist bei der ersten Konfiguration von IBM Firewall hilfreich. Durch diesen Konfigurationsassistenten steht einem Benutzer, der keine umfangreichen Kenntnisse über IBM Firewall besitzt, schon bald nach der Installation eine Basiskonfiguration zur Verfügung.

Network Security Auditor
: Der Network Security Auditor (NSA) überprüft die Netz-Server und IBM Firewall auf Lücken im Sicherheitssystem oder Konfigurationsfehler. Er ist schneller und zuverlässiger.

Neuerungen in MIMEsweeper für IBM SecureWay Release 2

Zu den Erweiterungen an MAILsweeper gehören:

- Nach Schlüsselwörtern suchen, um nicht der Netiquette entsprechende Post zu blockieren und wertvolle Daten gegen das Exportieren aus dem Unternehmen zu schützen.
- Ankommende Junk-E-Mail abwehren.
- Das Senden oder Empfangen bestimmter Arten von Dateien durch bestimmte Benutzer oder Gruppen blockieren.
- Dateien auf der Basis der Dateigröße blockieren oder verzögern, um eine Überlastung des Netzes zu vermeiden.

Zu den Erweiterungen an WEBsweeper gehören:

- Mitarbeitern den Zugriff auf Sites verwehren, die nicht arbeitsbezogen sind.
- Schutz gegen Attacken durch Extrahieren von Dokumenten über HTML- oder E-Mail-Adressen und von Site-Informationen über Cookies.

Neuerungen in SurfinGate

SurfinGate bietet die folgenden Erweiterungen:

- Prüfung des Inhalts von JavaScript-Code.
- Aufgabenkritische Leistungsüberwachung.
- Verbesserte Richtlinienverwaltung.
- Unterstützung für die Protokolle FTP und HTTPS.
- Plug-In-Integration mit Firewall-HTTP-Proxy.
- Die Fähigkeit, das Herunterladen bestimmter ausführbarer Dateien auf den Computer eines Benutzers zu blockieren.

Intrusion Immunity

Die Intrusion Immunity-Produkte enthalten jetzt Tivoli Cross-Site for Security.

Neuerungen in Tivoli Cross-Site for Security

Tivoli Cross-Site for Security erkennt Attacken auf die Systemsicherheit. Mit Tivoli Cross-Site for Security können Sie das Netz auf Attacken überwachen und die Integrität Ihres e-business sicherstellen.

Neuerungen in Norton AntiVirus Solution Suite

Norton AntiVirus Solution Suite Release 3.0.4 beinhaltet die folgenden aktualisierten Versionen:

- Norton AntiVirus 5.02 für Windows 95/98 und Windows NT Workstation
- Norton AntiVirus 5.02 für Windows NT Server
- Norton AntiVirus für IBM Operating System/2 (OS/2) 5.02
- Norton AntiVirus OS/2 für Lotus Notes 2.0
- Norton AntiVirus für Lotus Notes 2.0
- Norton AntiVirus für Microsoft Exchange 1.5.2

Public Key Infrastructure

Die Public Key Infrastructure-Komponente enthält jetzt Trust Authority. Trust Authority beinhaltet

- einen Installationsassistenten, der durch eine einfache Installation auf Windows NT führt.
- eine voreingestellte Konfiguration für den IBM 4758 Cryptographic Coprocessor. Sie können diese Konfiguration ändern.
- einen Konfigurationsassistenten, der die Gültigkeit der Daten überprüft, bevor die Programme für die Konfiguration im Hintergrund starten.
- Fehlernachrichte und Berichte.
- Online-Dokumentation einschließlich kontextbezogene Hilfe für Konfigurationsassistenten, Registration Authority Desktop und eine Client-Anwendung für End-Definitionseinheiten (End Entity, EE).

IBM SecureWay Toolbox

Die Toolbox bietet die folgenden Erweiterungen:

- Policy Director-APIs und Dokumentation.
- Verzeichnisservice-APIs.
- Public Key Infrastructure-APIs (PKIX-APIs) und Dokumentation.
- Der IBM Key Recovery Server 1.1.3.0 ist jetzt in der Toolbox enthalten. Er ist nur in Englisch verfügbar.

Teil 2. Gesichertes e-business-Netz planen

In Teil 2 wird die Planung für ein gesichertes e-business-Netz beschrieben.

In den folgenden Kapiteln wird typischer Internet-Datenverkehr und die Bedeutung der Sicherheit im Internet-Datenverkehr beschrieben. Anschließend wird gezeigt, wie FirstSecure-Produkte in einem e-business-Netz arbeiten.

Dieser Teil besteht aus den folgenden Kapiteln:

- Kapitel 3, „Übersicht über ein e-business-Netz“ auf Seite 19, enthält eine Beschreibung eines typischen e-business-Netzes und der in einem Netz vorhandenen Arten von Benutzern, Ressourcen und Interaktionen. Ein Netz kann zwar aus mehr oder weniger vielen Einrichtungen bestehen, die Bedeutung der Sicherheit und die Stufe des Sicherheitsschutzes hängt jedoch nicht von der Anzahl der Einrichtungen ab.
- In Kapitel 4, „FirstSecure im e-business-Netz planen“ auf Seite 31, wird gezeigt, wie die FirstSecure-Produkte in das Netz eingebunden werden können.
- Kapitel 5, „Policy Director im Netz planen“ auf Seite 33.
- Kapitel 6, „SecureWay Boundary Server im Netz planen“ auf Seite 37.
- Kapitel 7, „Intrusion Immunity im Netz planen“ auf Seite 45.
- Kapitel 8, „Public Key Infrastructure im Netz planen“ auf Seite 51.

Kapitel 3. Übersicht über ein e-business-Netz

Das e-business-Netz besteht aus Ressourcen, beispielsweise aus Daten und Datenbanken, Benutzern, Kunden, Lieferanten, Programmierern, Hardware, Unternehmensinformationen usw.. Nachfolgend werden einige dieser Bereiche untersucht, und es wird gezeigt, wo Sicherheit erforderlich ist.

Das Internet ist ein komplexes Gebilde. Der Datenverkehr durch das Internet fließt von Server zu Server und von Benutzer zu Benutzer in undefinierten Pfaden, die sich von Übertragung zu Übertragung ändern.

Die Übertragung Ihrer Geschäftsdaten über das Internet wird mit dem anderen Internet-Datenverkehr gemischt. Auf ihrem Weg können für Ihr Unternehmen wichtige Daten alle möglichen Server durchlaufen haben, und alle möglichen Internet-Benutzer können versucht haben, auf Ihre Ressourcen, Mitarbeiter und Daten zuzugreifen. Neben dem legitimen Datenverkehr beispielsweise für die Weiterbildung, das Geschäft oder auch nur zum Vergnügen werden im Internet auch Daten übertragen, die (absichtlich oder unabsichtlich) Schaden anrichten können. Abb. 1 auf Seite 20 enthält eine Übersicht über das Internet und zeigt, wie Ihr Datenverkehr das Internet zusammen mit dem Datenverkehr der anderen Internet-Teilnehmer durchläuft.

Mit FirstSecure können Sie Ihre Übertragungen sichern, indem Sie sie von dem gesamten anderen Datenverkehr trennen.

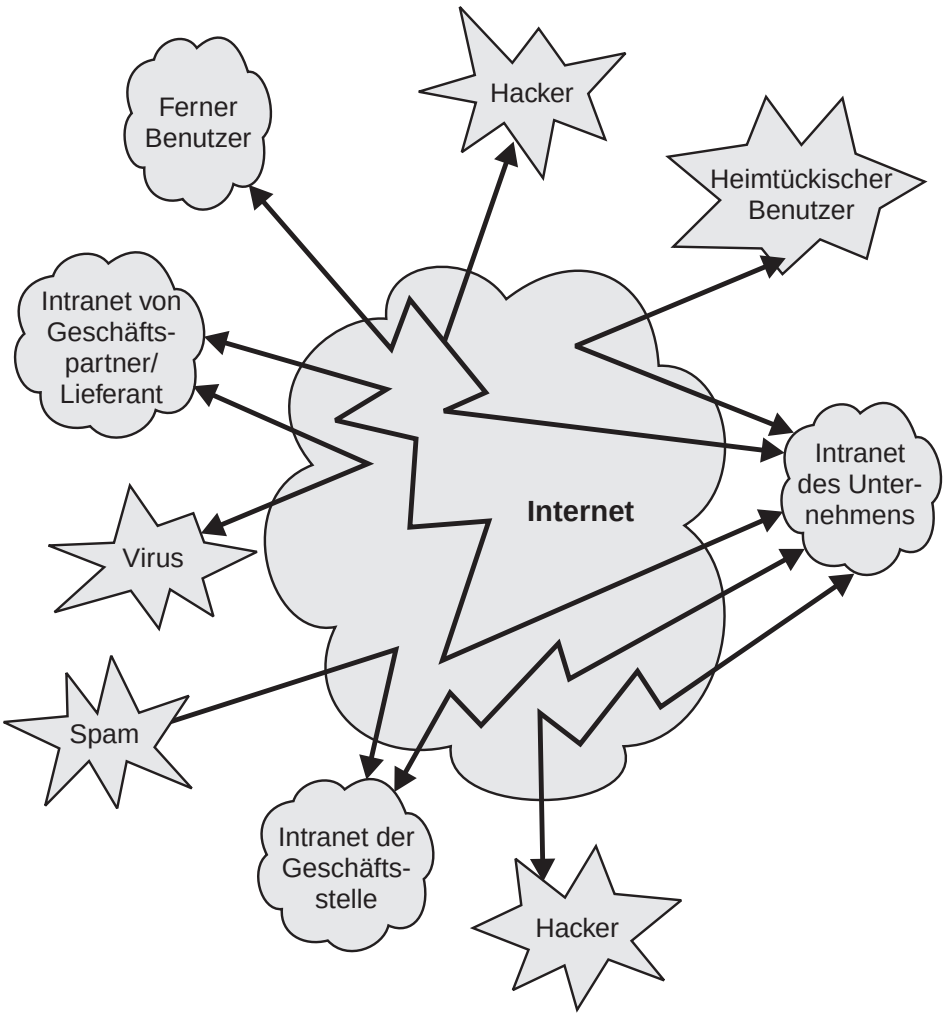


Abbildung 1. Übersicht über den Internet-Datenverkehr bei ungeregelten Aktivitäten

Sie wollen Ihren Internet-Datenverkehr natürlich nicht in einer solchen Internet-Umgebung abwickeln, sondern in der durch FirstSecure geschützten und in Abb. 2 auf Seite 21 dargestellten Umgebung.

Die ideale, durch FirstSecure geschützte Internet-Umgebung

Ein großer Teil ihres e-business-Datenverkehrs durchläuft das Internet. Sie wollen Ihre Transaktionen jedoch nicht in einer typischen Internet-Umgebung als eine umfangreiche Sammlung von beliebigen Daten abwickeln, die für fast alle Teilnehmer mit einem PC sichtbar sind. In Abb. 2 ist eine für Ihre Anforderungen geeignete, gesicherte Internet-Umgebung dargestellt.

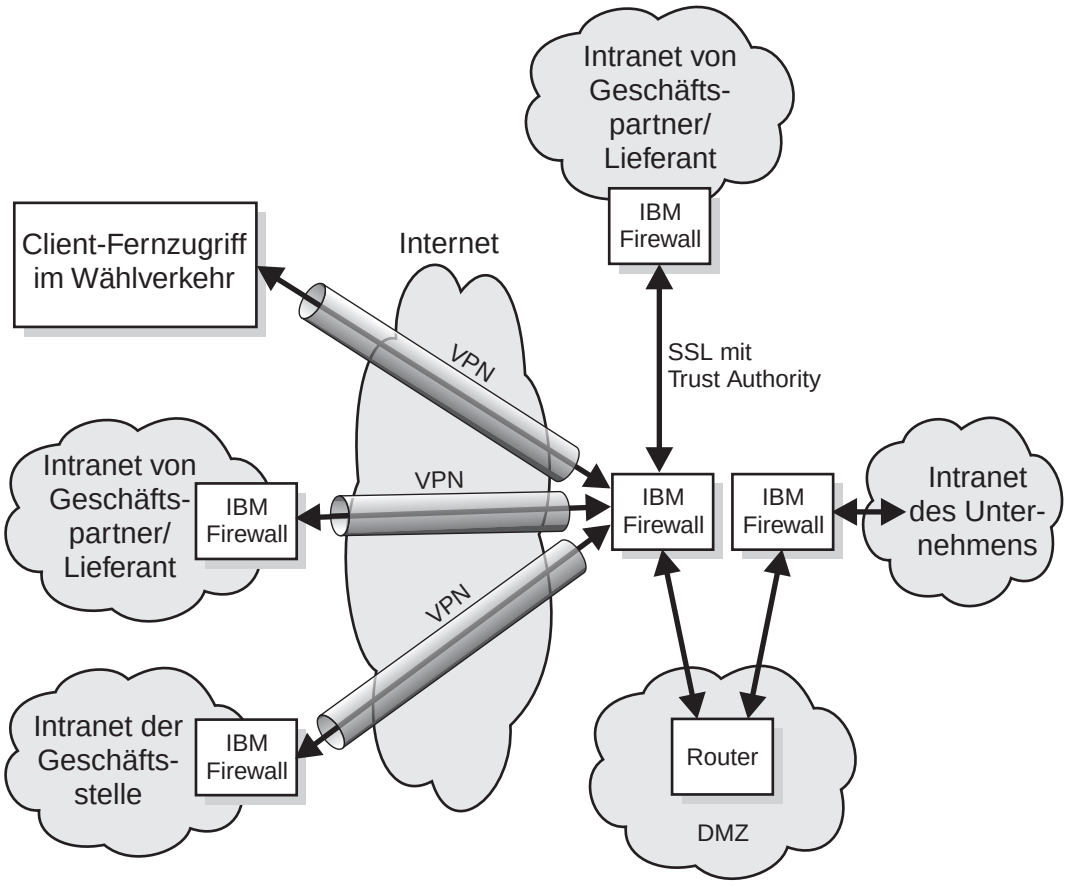


Abbildung 2. Gesicherte Internet-Umgebung

Zwar bietet das Internet eine umfangreiche Sammlung nützlicher Informationen, aber es sind auch Anwendungen, Daten und Teilnehmer vorhanden, gegen die Sie Ihr Netz abschirmen müssen. Sie müssen sicherstellen, daß

- Mitarbeiter nicht von ihren eigentlichen Aufgaben abgehalten werden.
- Mitarbeiter gegen die Zustellung unerwünschter E-Mail geschützt sind.
- sensible Geschäftsinformationen nicht nach außen gelangen können.

Das virtuelle private Netz

Ein virtuelles privates Netz (VPN) ist das Konzept einer privaten Verbindung über das Internet, auf die unerwünschte Personen oder Anwendungen keinen Zugriff haben. In Abb. 3 wird ein typisches virtuelles privates Netz gezeigt. Die Verbindung ist für die Benutzer an beiden Enden gegen das Eindringen unerwünschter Benutzer oder Anwendungen gesichert. FirstSecure-Produkte wie IBM SecureWay Firewall sind beim Aufbau und bei der Unterstützung virtueller privater Netze hilfreich.

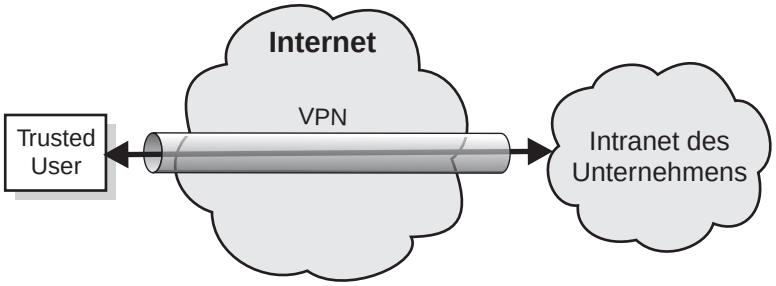


Abbildung 3. Typisches virtuelles privates Netz

DMZ (Demilitarized Zone)

In der *DMZ* (Demilitarized Zone) befinden sich die Ressourcen, auf die externe Benutzer zugreifen können. Mit IBM Firewall, MIMEsweeper und anderen FirstSecure-Produkten wird sichergestellt, daß nur befugte Benutzer auf die DMZ und auch nur auf bestimmte Ressourcen zugreifen können. Der Datenverkehr in die und aus der DMZ muß entsprechend überwacht werden.

Beispielsweise können Sie Ihren Unternehmenskatalog in die DMZ stellen, damit potentielle Kunden darauf zugreifen können, oder Sie können Broschüren mit Informationen über Ihr Unternehmen in die DMZ stellen. Die FirstSecure-Komponenten gewährleisten, daß nur Trusted User (authentifizierte Benutzer) auf die Informationen hinter der DMZ zugreifen können.

In Abb. 4 auf Seite 23 wird eine typische DMZ gezeigt.

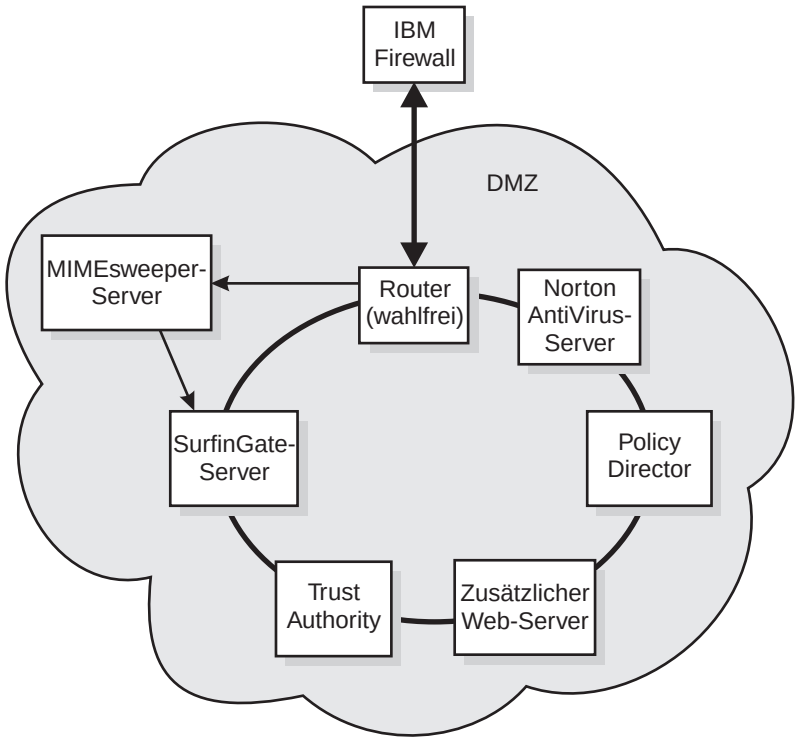


Abbildung 4. Typische DMZ mit Systemressourcen

Beim Entwickeln Ihrer gesicherten Anwendungen können Sie die DMZ als Basis für einen Intranet-Test verwenden, bevor Sie öffentliche Zugriffsberechtigung für diese Anwendungen erteilen.

Nachfolgend wird gezeigt, für welche Arten von Informationen Internet und Intranet benutzt werden.

Typisches Intranet eines Unternehmens

Über das Intranet des Unternehmens erfolgt die interne Kommunikation im Unternehmen. Es enthält Informationen und Ressourcen, die im Internet nicht zur Verfügung stehen. Ihre Mitarbeiter benutzen Daten gemeinsam, senden gegenseitig E-Mail und greifen auf Unternehmensressourcen wie Datenbanken, Drucker und Scanner zu. In Abb. 5 wird ein typisches Intranet eines Unternehmens gezeigt.

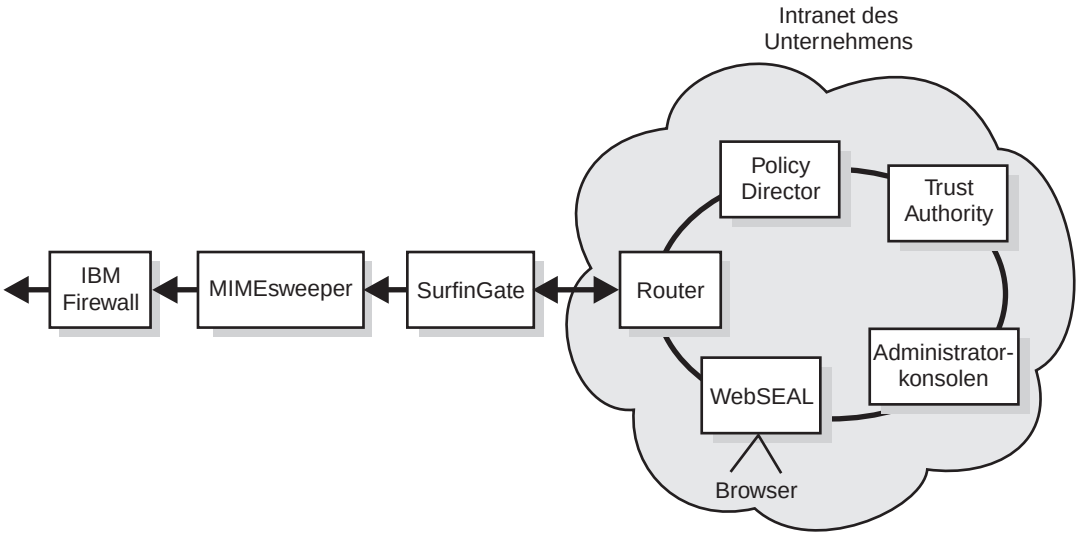


Abbildung 5. Übersicht über ein typisches Intranet eines Unternehmens

Sie müssen darauf achten, daß vertrauliche Unternehmensinformationen innerhalb Ihres Unternehmens bleiben und nur befugte Personen auf diese Daten zugreifen können. Es kann jedoch möglich sein, daß auf bestimmte Daten auch Kunden Zugriff haben sollen. Bankmitarbeiter sollen beispielsweise Kontostände, nicht aber persönliche Daten der Bankangestellten abfragen können. IBM Firewall sorgt dafür, daß persönliche Daten vertraulich bleiben.

IBM FirstSecure-Produkte helfen dabei, daß Ihr Intranet sicher ist. Mit dem Policy Director können Sie Zugriffsregeln festlegen. IBM SecureWay Trust Authority stellt die korrekte Identität der Benutzer sicher. Tivoli Cross-Site for Security informiert Sie über unbefugte Zugriffsversuche auf Ihre Intranet-Ressourcen.

Typisches Unternehmens-Intranet mit Geschäftsstellen

Mitarbeiter in fernen Geschäftsstellen müssen auf dieselben Daten und andere Ressourcen zugreifen können wie Mitarbeiter der Zentrale. Telefonleitungen zum Senden und Empfangen von Informationen sind jedoch langsam und gegen böswillige Störungen nicht geschützt. Sie wollen das Internet als kostengünstiges Mittel und als Mittel für einen zusätzlichen Schutz Ihrer Transaktionen einsetzen. In Abb. 6 wird eine typische Kommunikation zwischen einer Geschäftsstelle und der Zentrale über das Internet gezeigt.

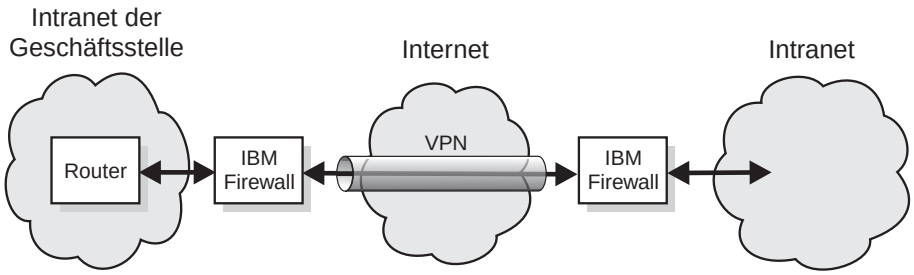


Abbildung 6. Über ein virtuelles privates Netz mit der Zentrale verbundene Geschäftsstelle

Sie wollen Ihre Übertragungen und Daten so sichern, als ob sie sich innerhalb eines einzigen Standorts befänden. Das *virtuelle private Netz* (VPN) ist Ihr Tunnel durch das Internet. Sie benutzen das Internet wie ein privates Intranet-Netz.

Ein typischer Mitarbeiter mit Fernzugriff

Wenn einige Ihrer Mitarbeiter zeitweise oder permanent außerhalb der Zentrale arbeiten, können sie über eine Wähl- oder Standleitung über das Internet auf Ihr Netz zugreifen.

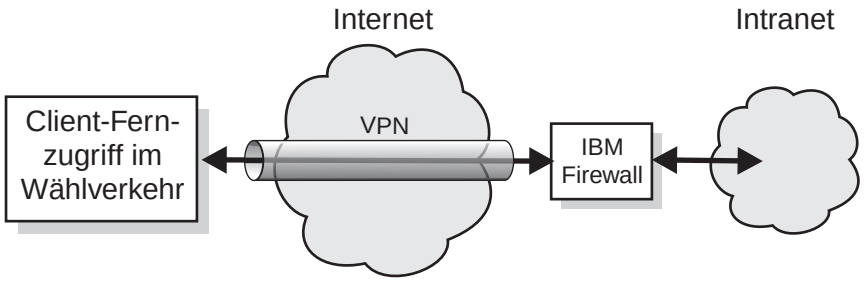


Abbildung 7. Client, der mit einer Wählleitung über ein virtuelles privates Netz per Fernzugriff auf die Zentrale zugreift.

IBM Firewall schützt die Übertragungen dieses Mitarbeiters.

Typisches Intranet eines Geschäftspartners oder Lieferanten

Ihr Geschäft ist effizienter, wenn Ihre Geschäftspartner und Lieferanten auf einige Ihrer Daten direkt zugreifen können. Beispielsweise kann ein Lieferant berechtigt werden, Ihren Lagerbestand zu überprüfen, damit er neue Ware sendet, wenn ein bestimmter Bestand unterschritten wird. Einem anderen Geschäftspartner kann Zugriff auf andere ausgewählte Sätze erteilt werden. Eine Abrechnungsfirma benötigt möglicherweise Zugriff auf Sätze mit Steuerdaten, nicht aber auf die Sätze mit Informationen über Geschäftspartner. In Abb. 8 und Abb. 9 wird ein typischer Lieferant oder Geschäftspartner gezeigt. Sie wollen, daß Geschäftstransaktionen das Internet so durchlaufen, als ob sie eine private Verbindung durchlaufen würden.

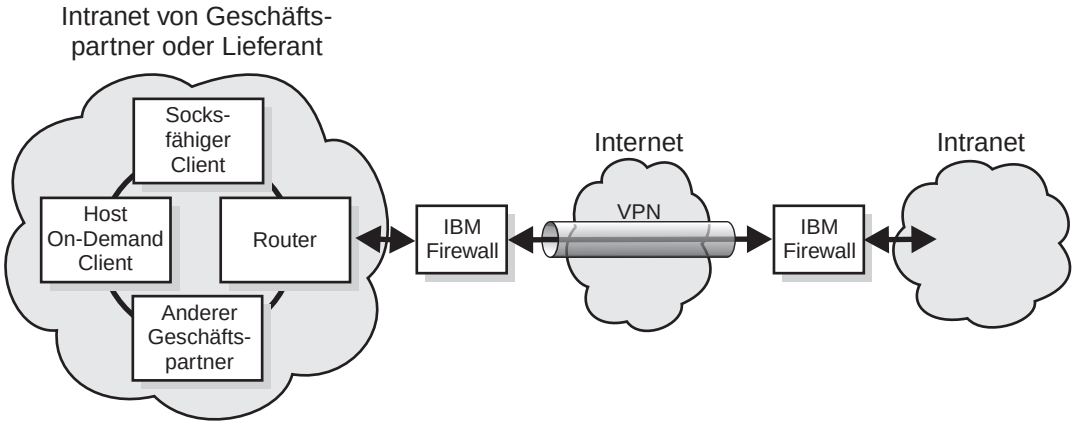


Abbildung 8. Typisches Intranet eines Geschäftspartners oder Lieferanten, der ein virtuelles privates Netz benutzt

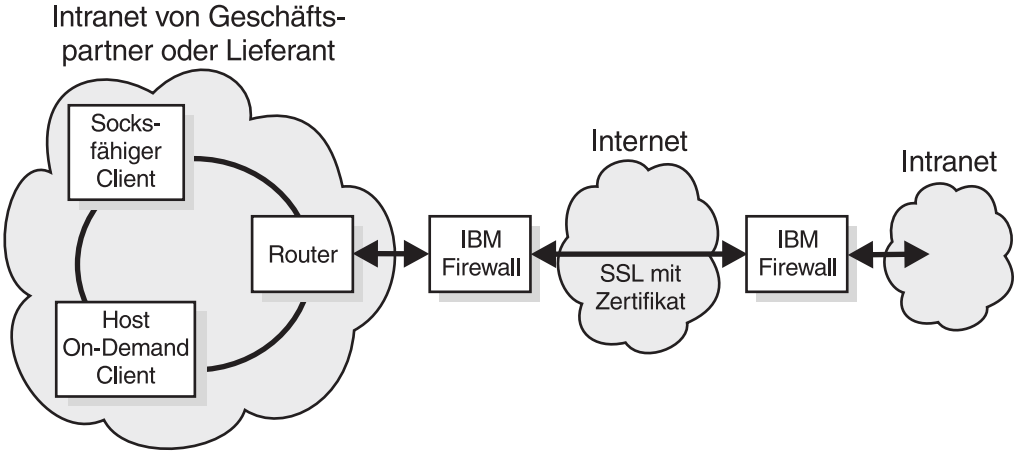


Abbildung 9. Typisches Intranet eines Geschäftspartners oder Lieferanten, der ein SSL-Übertragungsprotokoll benutzt

Dieser Geschäftspartner benutzt statt eines virtuellen privaten Netzes das Protokoll SSL (Secure Sockets Layer), da die Übertragungen von einem Ende zum anderen Ende verschlüsselt werden. (Der Benutzer kann als zusätzliche Sicherheit auch noch ein virtuelles privates Netz verwenden.)

Sie müssen diese Benutzer voreinander und gegen böswillige Störungen und Eindringlinge schützen. Sie müssen ihre Datenübertragungen gegen unbefugte Empfänger und Absender schützen. Zudem müssen Sie sicherstellen, daß diese Benutzer nur auf die Daten zugreifen können, auf die sie zugreifen dürfen. Auch müssen Sie sicherstellen, daß die Identität dieser Benutzer überprüft werden kann.

Daten und Datenbanken

Daten gehören zu den wertvollsten Ressourcen von Unternehmen. Bestimmte e-business-Daten sollen für alle Internet-Benutzer zugänglich sein. Beispielsweise kann ein Hardware-Verteiler Bestands- und Preislisten für den Online-Einkauf bereitstellen. Ein Bekleidungsgeschäft kann einen illustrierten Online-Katalog mit Formen, Farben und Größen für den Online-Einkauf bereitstellen.

Bevor Sie Zugriff auf Daten erteilen, müssen Sie wissen, wer die Daten anfordert und warum die Daten angefordert werden. Benutzen Sie Trust Authority zum Ausgeben von Zertifikaten an Trusted User (authentifizierte Benutzer).

Weitere zu schützende Bereiche

In diesem Buch wird nicht auf Gegenmaßnahmen für andere Sicherheitsbereiche eingegangen. Sie müssen auch folgendes planen:

- Standortsicherheit, Erteilung und Entzug des Zugriffs auf den Standort, Aufsplitterung des Standorts.
- Physische Sicherheit von Laptop-Computern, Personal Computern und Workstations und anderen Containern.
- Überprüfung des persönlichen Hintergrunds auf eventuelle Sicherheitsrisiken.
- Ablehnungserklärungen für Haftung, Verträge usw..
- Betriebspraktiken wie Schlüsselverwaltung, Informationssteuerung und Informationen und Schulungen bezüglich der Sicherheit.

Betriebssystem

Die meisten Betriebssysteme sind so konfiguriert, daß sie eine hohe Verfügbarkeit und umfangreiche Funktionen bieten. Ein effektives Sicherheitskonzept beinhaltet beispielsweise, daß für eine bestimmte Aufgabe nur das Minimum an erforderlichen Funktionen zur Verfügung steht. Sie sollten in Erwägung ziehen, alle Betriebssystemfunktionen zu deinstallieren oder zu inaktivieren, auf die Eindringlinge keinen Zugriff haben dürfen.

Typische Benutzer

Im Internet gibt es verschiedene Arten von Benutzern, teils mit guten, teils mit schlechten Absichten. Im e-business sollen Benutzer Kunden sein und online einkaufen und nach Informationen suchen können. Im e-business sollen Geschäftspartner auf bestimmte Daten zugreifen können, um beispielsweise den Bestand zu überprüfen, Entscheidungen zur Fertigung zu treffen oder Kommentare zu Plänen und Aktivitäten innerhalb des Geschäfts abzugeben. Im e-business sollen Mitarbeiter auf die Daten zugreifen können, die sie zur Ausführung ihrer Aufgaben benötigen.

Im Internet tummeln sich jedoch auch Benutzer, die kein e-business will: Hacker, Spammer (Benutzer, die unerwünschte E-Mail verschicken), Benutzer, die Viren verbreiten, Benutzer, die auf sensible Daten zugreifen wollen. Diese Benutzer befinden sich möglicherweise sogar innerhalb Ihres e-business.

Bevor Sie Zugriff auf eine Ressource erteilen, müssen Sie wissen, welcher Benutzer die Ressource anfordert, welchen Zugriff dieser Benutzer auf Daten und Anwendungen haben darf und welche Aufzeichnungen über den Benutzerzugriff aufbewahrt werden sollen.

Anwendungen und Anwendungserstellung

Anwendungen können so entworfen werden, daß die Sicherheit berücksichtigt wird. Sie können die Verschlüsselung der zu übertragenden Daten, die Zertifizierung von Benutzern, die Zugriff anfordern, und Prüfprotokolle von Benutzern und Transaktionen nutzen.

Die Sicherheit kann über die Toolbox-APIs in Ihre Anwendungen integriert werden.

Sicherheit der Hardware

Server und Datenbanken sind Teil eines gesicherten Systems. Die Sicherheit der Hardware wird in diesem Buch zwar nicht behandelt, Sie müssen jedoch einen Plan für die physische Sicherheit von Servern und für die Workstations erstellen, die für die Verwaltung der Sicherheit benutzt werden.

Sicherheit der Hardware mit Trust Authority

Zwar bezieht sich dieser Abschnitt speziell auf die Komponente Trust Authority, die Überlegungen gelten jedoch für alle FirstSecure-Komponenten.

Isolierung des Bereichs
: Installieren Sie den Server in einem separaten Raum, der ausschließlich für die Zertifizierungsstelle reserviert ist. Falls möglich, sollte der Raum verstärkte Wände, eine solide Holz- oder Stahltür und einen soliden Fußboden haben. Zudem sollte der Raum als Schutz gegen Entladung bei einem Feuer über einen Doppelboden verfügen.

Pflege des Bereichs
: Die im Raum befindlichen Computer sollten über eine unterbrechungsfreie Stromversorgung verfügen. Zudem sollte der Raum über fest angebrachte Lichtquellen, Bewegungsdetektoren und Wärme- und Kühlsystem verfügen. Zudem muß auf eine ordnungsgemäße Belüftung des Raumes geachtet werden, damit die durch die Geräte entstehende Wärme abziehen kann.

Steuerung der Zugangsberechtigung für den Bereich
: Die Zugangsberechtigung für den physischen Bereich kann auf mehrere Arten erteilt werden, beispielsweise durch Ausweisleser oder die Eingabe von Codes. Um zu verhindern, daß sich eine unbefugte Person durch Manipulation Zugang verschafft, sollten Sie Kontrollen installieren, bei denen mindestens zwei authentifizierte Personen die entsprechenden Zugangsberechtigungen präsentieren müssen.

Zudem sollten Sie den Raum überwachen, damit Sie feststellen können, wann und von wem der Raum betreten wurde. Installieren Sie zur Optimierung der Sicherheit Bewegungsdetektoren sowohl innerhalb als auch außerhalb der Tür.

DFV-Steuerung

Auf dem Trust Authority-Server sollten keine offenen Ersatzanschlüsse vorhanden sein. Sie sollten das System so konfigurieren, daß nur Anforderungen auf den Anschlüssen akzeptiert werden, die den aktiven Trust Authority-Anwendungen explizit zugeordnet sind.

Gehen Sie anhand Ihrer im Unternehmen üblichen Prozeduren und Anforderungen vor, um die im e-business benutzte Hardware zu sichern.

Kapitel 4. FirstSecure im e-business-Netz planen

In den folgenden Kapiteln wird gezeigt, wie die FirstSecure-Produkte in das e-business eingebunden werden können. Die Kapitel bauen auf den Abbildungen in Kapitel 3, „Übersicht über ein e-business-Netz“ auf Seite 19, auf. Jedes Produkt wird näher beschrieben. Vollständige Informationen über ein Produkt enthält die mit dem Produkt gelieferte Dokumentation. Die Szenarien für die Nutzung sind lediglich Vorschläge.

In allen Szenarien für die Nutzung führen Sie dieselben grundlegenden Schritte aus:

1. Sorgen Sie dafür, daß alle Teile des Netzes dieselbe Zeitreferenz verwenden, damit die Prüfprotokolle vereinfacht werden und genauer sind.
2. Installieren und testen Sie Komponenten zunächst in Ihrem Intranet.
3. Wurden die Komponenten im Intranet installiert und getestet, bauen Sie Anwendungen innerhalb der gesicherten DMZ (Demilitarized Zone) auf.
4. Der Datenverkehr zwischen dem Intranet und der DMZ muß eine Firewall durchlaufen.
5. Bauen Sie externe Anwendungen auf und testen Sie diese mit Testdaten.
6. Installieren Sie eine Firewall, um den Datenverkehr zwischen Internet und DMZ zu schützen.
7. Gewähren Sie Benutzern den Zugriff auf das Netz.

Vollständiges FirstSecure-System planen

Nachfolgend wird vorgeschlagen, in welcher Reihenfolge vorgegangen werden kann, um die FirstSecure-Produkte im Netz zu nutzen. Diese Darstellung ist stark vereinfacht. In Teil 3, „Voraussetzungen für die Installation und Integration“ auf Seite 57, sind die Hardware- und Softwarevoraussetzungen für die einzelnen Produkte und Überlegungen zur Integration aufgeführt. Lesen Sie zudem die Informationen über Voraussetzungen und Anweisungen zur Installation, die den einzelnen Produkten beiliegen. Für viele Produkte sind zudem neueste Informationen im Internet verfügbar.

In „Web-Informationen“ auf Seite xii sind die Web-Sites mit FirstSecure-Informationen aufgeführt. Das Redbook *Understanding the IBM SecureWay FirstSecure Framework*, IBM Form SG24-5498, enthält mehrere ausführliche Szenarien.

1. Stellen Sie fest, welche Sicherheitsvoraussetzungen erforderlich sind.
2. Installieren Sie den Policy Director so, daß diese Anforderungen erfüllt werden.
3. Erstellen und testen Sie die Kunden-Server-Anwendung zunächst innerhalb Ihres Intranets, stellen Sie sie noch nicht im Internet zur Verfügung.
4. Installieren Sie IBM Firewall zum Schutz der Kunden-Server-Anwendung.
5. Fügen Sie der DMZ das Produkt SurfinGate hinzu.
6. Fügen Sie der DMZ die Produkte MIMEsweeper und Norton AntiVirus hinzu, um die Anwendungen zu schützen, wenn Sie sie im Internet zur Verfügung stellen. Wenn Sie die Anwendungen für den externen Datenverkehr zur Verfügung stellen, konfigurieren Sie die Anwendungen so, daß sie auf Ihre Server zeigen.
7. Installieren Sie das Produkt Tivoli Cross-Site for Security als Schutz gegen Attacken auf das System und zum Erkennen solcher Attacken.
8. Fügen Sie innerhalb der DMZ folgendes hinzu:
   - Web-Server
   - Web-Katalog-Server
   - Web-Inventar-Server
   - Kunden-Client-Anwendungen
   - Gesicherte Kunden-Client-Anwendungen
   - Mindestens einen Cross-Site for Security-Agent

   Testen Sie alle Anwendungen innerhalb der Firewall, bevor Sie sie für den Datenverkehr öffnen. Benutzen Sie das SecureWay Boundary Server-Tool Network Security Auditor (NSA), um die festgelegten Regeln zu testen.
9. Installieren Sie ein IBM SecureWay Firewall-Exemplar, um die Software innerhalb der DMZ zu schützen. Die Standardkonfiguration darf keinen Datenverkehr zulassen, damit Sie die Installation testen können, bevor Sie sie für die Allgemeinheit zugänglich machen.
10. Installieren Sie Trust Authority und geben Sie Zertifikate an Trusted User (authentifizierte Benutzer) aus.
11. Stellen Sie die Anwendung im Internet zur Verfügung, nachdem alle Tests abgeschlossen sind.
12. Führen Sie den Network Security Auditor außerhalb Ihres Systems aus, damit Sie die Regeln testen können, bevor Sie der Allgemeinheit den Zugang ankündigen.
13. Überprüfen Sie die von den FirstSecure-Komponenten erstellten Prüfprotokolle, um festzustellen, ob unerwünschte Ereignisse aufgetreten sind.
14. Setzen Sie die Überprüfung der Prüfprotokolle fort und fügen Sie Cross-Site for Security-Agents hinzu, wenn Sie dem Netz Anwendungen hinzufügen.

Kapitel 5. Policy Director im Netz planen

FirstSecure liefert einen konsolidierten Steuerungspunkt für heterogene Web-Umgebungen auf der Basis der Sicherheitsrichtlinien im Unternehmen. In Umgebungen, in denen Benutzer über Browser auf mehrere Backend-Web-Server zugreifen, bietet der Policy Director folgendes:

- Eine einstufige Anmeldung für jeden Web-Benutzer.
- Identifikationsprüfung.
- Berechtigungsprüfung von Benutzern, die Zugriff auf geschützte Web-Seiten anfordern.

Mit dieser Unterstützung können Sie den Zugriff auf folgendes steuern:

- TCP/IP-Austausch, beispielsweise HTML, Telnet und POP3
- Anwendungen anderer Anbieter, z. B. Datenbanksysteme
- Netzverwaltungs-Tools
- Unternehmensinterne Anwendungen

Mit FirstSecure erfolgt die Authentifizierung von Benutzern für den Policy Director über die folgenden Mechanismen:

- Basisauthentifizierung über SSL (Secure Sockets Layer)
- Formulargestützte Anmeldung über SSL
- SSL mit Client-Zertifikaten
- Kerberos-Anmeldung

FirstSecure steuert dann den Zugriff von authentifizierten Benutzern auf einzelne Web-Objekte und Netzservices. Für nicht authentifizierte Benutzer kann der Zugriff auf eine Untergruppe dieser Ressourcen begrenzt werden.

Einsatz von Policy Director

Policy Director verwaltet die Zuordnung zwischen Benutzern und Gruppen einerseits und Ressourcen andererseits. Über die Policy Director-Verwaltungskonsole (Management Console) können Sie folgendes:

- Benutzer und Gruppen definieren, die Ihre Ressourcen verwenden.
- Zu schützende Objekte definieren. Zu diesen Objekten können das Web, TCP-Anschlüsse, Methoden und Schnittstellen gehören.
- Die Art des Zugriffs von Benutzern auf Ressourcen definieren und festlegen, über welche Regeln die Ressourcen geschützt werden sollen (beispielsweise Lesen, Ändern, Verwalten, Ausführen oder Löschen).

In der folgenden Tabelle werden die allgemeinen Konfigurationen von Policy Director-Komponenten beschrieben. Ermitteln Sie die für Ihr Netz geeignete Konfiguration. Wählen Sie diese Komponenten während der Installation aus.

Weitere Informationen enthält das Buch *IBM SecureWay Policy Director Installation und Konfiguration*.

Konfigurationsbeispiel	**Installierte Komponenten**
Ein Server mit dem einzigen Exemplar des Verwaltungs-Servers für die gesicherte Domäne. In diesem Szenario befindet sich der Verwaltungs-Server auf seinem eigenen System. Der Verwaltungs-Server pflegt die Berechtigungsstammdatenbank für die gesicherte Domäne, vervielfältigt diese Datenbank in der gesicherten Domäne und pflegt Positionsinformationen über andere Policy Director-Server-Maschinen in der gesicherten Domäne.	Nur Verwaltungs-Server
WebSEAL-Server. Dieses Szenario stellt die Lösung zum Schutz eines Web-Speicherbereichs dar. WebSEAL unterstützt Backend-Server, damit eine hohe Verfügbarkeit und Fehlertoleranz gegeben ist.	Security Manager mit WebSEAL
NetSEAL-Server. Dieses Szenario stellt die Lösung zum Sichern eines virtuellen privaten Netzes dar und bietet Zugriffssteuerung für vorhandene Netzservices und Netzservices anderer Anbieter.	Security Manager mit NetSEAL
Ein kombinierter WebSEAL- und NetSEAL-Server.	Security Manager mit WebSEAL und NetSEAL
Ein Server, durch den Anwendungen anderer Anbieter auf den Policy Director-Berechtigungsservice (Authorization Service) zugreifen können.	Berechtigungs-Server
Ein Server, der eine Entwicklungsumgebung für Entwickler bietet, die Anwendungen anderer Anbieter aufbauen wollen, die die Berechtigungs-API benutzen.	Berechtigungs-Server und ADK
Ein Server, der die kombinierten Services aller oben aufgeführten Konfigurationen bietet.	Alle Komponenten

Der Policy Director ist ein weit verbreitetes Sicherheitssystem, dessen Komponenten in einer Vielzahl von Konfigurationen auf einer oder mehreren Maschinen eingesetzt werden können. Nachfolgend wird eine Übersicht über den Einsatz von Policy Director in Ihrem Netz gegeben. Vollständige Installationsanweisungen befinden sich im Buch *IBM SecureWay Policy Director Installation und Konfiguration*.

1. Installieren Sie den Policy Director-Sicherheits-Server.

   Mindestens ein Computer in der gesicherten Domäne muß den Policy Director-Sicherheits-Server enthalten, damit eine gesicherte Policy Director-Domäne aufgebaut werden kann. Weitere Informationen können Sie den Installations- und Verwaltungshandbüchern für die erforderlichen Plattformen entnehmen, oder bitten Sie die entsprechende technische Unterstützung um Hilfe.

   Für die restlichen Server sind nur DCE-Client-Installationen erforderlich (oder NetSEAT auf Windows NT-Systemen).
2. Installieren Sie den LDAP-Server.
3. Installieren Sie den Policy Director.
   - Der Policy Director-Sicherheits-Server muß zuerst installiert werden (siehe Schritt 1).
   - Für alle Policy Director-Server-Installationen ist das Policy Director-Basisprodukt erforderlich.
   - Handelt es sich um die *erste* oder *einzige* Maschine in der gesicherten Domäne, muß der Verwaltungs-Server installiert werden.

     Handelt es sich um eine *zusätzliche* Maschine in einer vorhandenen gesicherten Domäne mit einem vorhandenen Verwaltungs-Server, installieren Sie keinen weiteren Verwaltungs-Server. In einer gesicherten Domäne darf nur ein einziges Exemplar des Verwaltungs-Servers vorhanden sein.
   - WebSEAL, NetSEAL und Berechtigungs-Server-Komponenten anderer Anbieter sind wahlfrei.
   - Der Security Manager wird mit WebSEAL kombiniert, damit die WebSEAL-HTTP-Server-Komponente und eine feingliedrige HTTP-Zugriffssteuerung verfügbar ist. Er wird zudem mit NetSEAL kombiniert, damit die grobgliedrige NetSEAL-TCP/IP-Zugriffssteuerungs.-komponente verfügbar ist.

4. Installieren Sie die Verwaltungskonsole (Management Console).

   Für die Verwaltungskonsole (Management Console) muß ein DCE-Client (oder NetSEAT für Windows NT) auf dem Betriebssystem installiert werden (siehe Schritt 1 auf Seite 35).

5. Für Anwendungen, die mit dem Berechtigungs-ADK entwickelt wurden, gelten folgende Abhängigkeiten:
   - Das Policy Director-Paket ist erforderlich.
   - Installieren Sie IVAuthADK auf der Anwendungsmaschine.
   - Auf dem Betriebssystem, auf dem die Anwendungen laufen, muß ein DCE-Client installiert sein. Bei einem Windows NT-System muß NetSEAT installiert sein.
   - Auf mindestens einem Computer in der gesicherten Domäne muß ein Berechtigungs-Server installiert sein, damit die gesicherte Domäne eine Anwendung ausführen kann. In einer typischen Entwicklungsumgebung befindet sich der Berechtigungs-Server auf demselben Betriebssystem wie das Berechtigungs-ADK.

Kapitel 6. SecureWay Boundary Server im Netz planen

FirstSecure bietet Sicherheit für web-gestützte Anwendungen, die die Vorteile der vorhandenen Sicherheitsstandards wie SSL (Secure Sockets Layer), SOCKS und IPSec nutzen.

Beinhaltet die Betriebsumgebung Verbindungen zwischen zwei Teilen des Netzes mit unterschiedlichen Sicherheitsmerkmalen, können mit der FirstSecure-Komponente SecureWay Boundary Server die folgenden Anforderungen erfüllt werden:

- Sichere Verbindungen zum Internet und Minimierung der Gefahr eines unbefugten Zugriffs auf das private Netz.
- Umfangreiche Extranet-Infrastrukturen für die selektive gemeinsame Datennutzung mit Geschäftspartnern und Lieferanten.
- Benutzung des Internet oder anderer relativ ungesicherter Netzsegmente als virtuelles privates Netz (VPN), bei dem die Vertraulichkeit der Nachrichten auch beim Durchlaufen der Infrastruktur des ungesicherten Netzes erhalten bleibt.

Die FirstSecure-Komponente SecureWay Boundary Server benutzt Netzadressenfilter, Inhaltsfilter, Proxies und Circuit-Level-Gateways. Durch die Kombination dieser Technologien ermöglicht SecureWay Boundary Server sichere e-business-Operationen auf der Basis der Sicherheitsrichtlinien im Unternehmen, indem die Kommunikation zwischen Netzen mit unterschiedlichen Sicherheitsmerkmalen gesteuert wird.

SecureWay Boundary Server beinhaltet folgendes:

- IBM SecureWay Firewall, einschließlich ACE/Server
- MIMEsweeper für IBM SecureWay Release 2
- SurfinGate 4.05 für Windows NT
- Verbesserte Richtlinienverwaltung

Eine Übersicht über den Datenfluß in einer vollständigen SecureWay Boundary Server-Installation enthält Abb. 10.

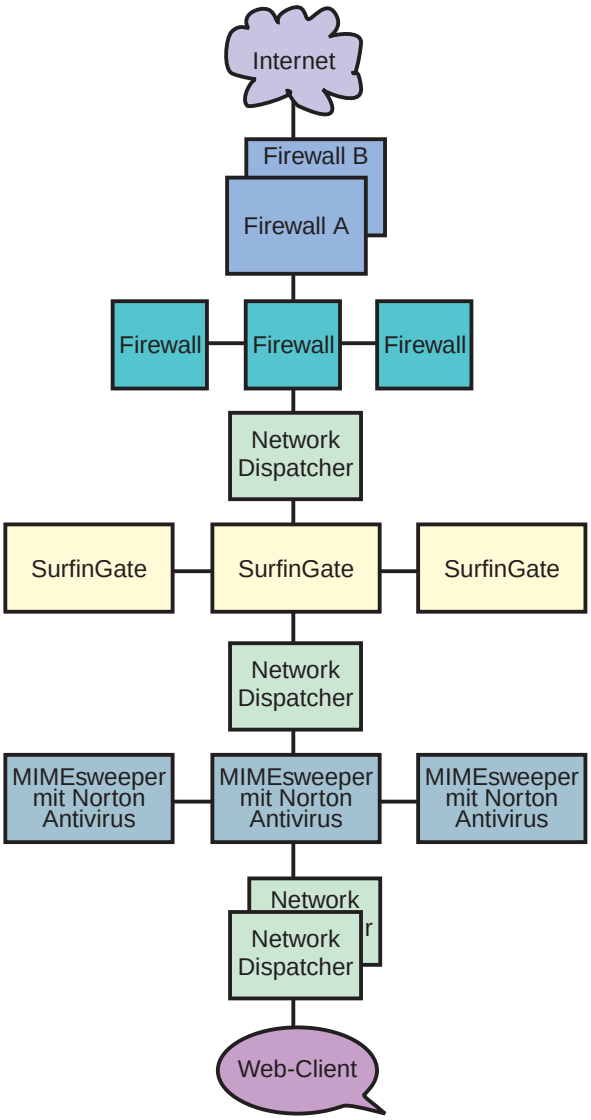


Abbildung 10. Übersicht über den Datenfluß in SecureWay Boundary Server-Produkten

Einsatz von IBM SecureWay Firewall

IBM SecureWay Firewall, auch als IBM Firewall bezeichnet, steuert Übertragungen in das und aus dem Internet. Diese Firewall-Technologie schützt auch die IBM Ressourcen.

Überlegungen hinsichtlich der Installation stehen in „Überlegungen zu den SecureWay Boundary Server-Komponenten“ auf Seite 67.

Hinsichtlich des Netzbetriebs können folgende Bedenken auftreten:

- Unbefugter Zugriff auf das Netz, die Anwendungen und die Daten des Unternehmens beim Anschluß an das Internet.
- Mißbrauch der Netzressourcen des Unternehmens durch interne Benutzer.
- Hohe Kosten für die Verwaltung der Konfiguration einer umfangreichen Extranet-Infrastruktur für Geschäftspartner und Lieferanten.
- Hohe Kosten für Standleitungen zwischen Geschäftsstellen.
- Geringe Produktivität durch ineffektive, verzögerte oder mißverständliche Kommunikation mit Geschäftspartnern und Lieferanten.
- Hohe Kosten für die Verwaltung von Software in anderen Landessprachen.

IBM Firewall kann diese Bedenken zerstreuen. Da nur explizit zugelassener Datenverkehr die Firewall passieren kann, schützt IBM Firewall das Netz gegen unbefugtes Eindringen. Zudem verfügt IBM Firewall über Software zum Aufdecken von Schwachstellen, durch die die Sicherheit des Servers, auf dem IBM Firewall läuft, gegen unbefugtes Eindringen erhöht wird. Die IP-Adressen und die Konfiguration des internen Netzes sind vom ungesicherten Netz aus nicht erkennbar. Der gesamte Datenverkehr über die Firewall wird protokolliert und kann zum Generieren von Berichten über Benutzeraktivitäten verwendet werden.

IBM Firewall und die IBM Firewall-VPN-Konfigurationsanwendung ermöglichen die Nutzung und kostengünstige Verwaltung umfangreicher VPN-Infrastrukturen. Netzstudien haben ergeben, daß die Nutzung virtueller privater Netze im Vergleich zu Standleitungen erheblich kostengünstiger ist. Mit IBM Firewall können Geschäftsstellen über das Internet miteinander verbunden werden, indem in allen Geschäftsstellen Firewalls eingesetzt werden und ein IPSec-gestützter Tunnel verwendet wird.

Mit IBM Firewall wird der ACE/Server geliefert. Der ACE/Server ist ein Produkt der Security Dynamics Technologies, Inc.. Er bietet leistungsfähige, zentralisierte Authentifizierungsservices für Unternehmensnetze, damit nur befugte Benutzer auf Netzdateien, Anwendungen und DFV-Funktionen zugreifen können. In Kombination mit der patentierten SecurID-Token-Technologie von Security Dynamics Technologies Inc. errichtet der ACE/Server eine Barriere gegen unbefugten Zugriff. Die Authentifizierung basiert auf zwei Faktoren: Benutzer müssen für die Authentifizierung *etwas haben* (eine SecurID-Token-Karte) und *etwas wissen* (eine PIN-Nummer).

Einsatz von MIMEsweeper

MIMEsweeper, ein Produkt der Content Technologies Ltd., analysiert Internet- und Intranet-Daten auf der Basis ihres Inhalts, um versteckte Gefahrenquellen aufzudecken und die Netzbenutzer gegen solche Gefahrenquellen zu schützen.

Überlegungen hinsichtlich der Installation stehen in „Überlegungen zu den SecureWay Boundary Server-Komponenten“ auf Seite 67.

MIMEsweeper enthält die beiden Basismodule MAILsweeper und WEBsweeper, die die Benutzer auf unterschiedliche Arten schützen. Wenn E-Mail und andere Web-Daten MIMEsweeper erreichen, überprüft MIMEsweeper die Adresse des Absenders und des Empfängers und zerlegt die Dateien dann rekursiv in ihre Einzelteile. MAILsweeper und WEBsweeper analysieren diese Teile dann, um das Risiko, daß versteckte Gefahrenquellen in das private Netz eindringen können, zu verringern.

FirstSecure beinhaltet MAILsweeper 4.0 und WEBsweeper 3.2_5. Diese Produkte können separat installiert, konfiguriert und benutzt werden.

MAILsweeper kann folgendes:

- Mit ausgewählten Virenprüfprogrammen arbeiten, um die zerlegten Dateien auf Viren zu untersuchen.
- Makrobomben erkennen und abwehren.
- Nach Schlüsselwörtern suchen, um folgendes zu verhindern:
  - Die Übertragung von E-Mail, deren Inhalt gegen die Netiquette verstößt.
  - Die Übertragung von Unternehmensdaten an unbefugte Stellen.
- Spam-E-Mail abwehren, um das Netz zu entlasten und einen Produktivitätsverlust der Mitarbeiter zu verhindern.
- Das Senden oder Empfangen bestimmter Arten von Dateien (z. B. AVI-Dateien oder MPEG-Dateien) durch bestimmte Benutzer oder Gruppen blockieren.
- Dateien auf der Basis der Dateigröße blockieren oder verzögern, bis das Netz den Datenverkehr besser bearbeiten kann.

WEBsweeper kann folgendes:

- Die Kommunikation der Mitarbeiter mit bestimmten Sites blockieren, die nicht arbeitsbezogen sind.
- Vertrauliche und sensible Dokumente gegen versehentlichen Verlust schützen.

Zudem enthält MIMEsweeper eine Anwendungsprogrammierschnittstelle (API), die zur Integration von URL-Blockern anderer Anbieter benutzt werden kann.

MIMEsweeper kann ein wichtiges Element zum Schutz des Unternehmens und der Benutzer gegen Sicherheitsrisiken aus dem Internet sein.

Anmerkung: Möglicherweise enthält die MIMEsweeper-Dokumentation Informationen über die Kontaktaufnahme mit Content Technologies, wenn Service und Unterstützung benötigt werden. Wird MIMEsweeper für IBM SecureWay Release 2 jedoch als Teil des Angebots SecureWay FirstSecure oder SecureWay Boundary Server geliefert, muß Kontakt mit IBM aufgenommen werden, wenn Service und Unterstützung benötigt werden.

Einsatz von SurfinGate

SurfinGate, ein Produkt der Finjan Software Ltd., untersucht mobilen Code, z. B. JavaScript-Code, Java-Minianwendungen und ActiveX-Steuerungen, um das Netz gegen Schäden wie Datenmodifizierung, Löschen von Informationen oder illegales Sammeln von Informationen zu schützen. SurfinGate untersucht mobilen Code auf Gateway-Ebene und erkennt Code, der eine Gefahrenquelle darstellt, bevor dieser Code in das Netz eindringt. Mobiler Code kann selektiv für bestimmte Benutzer oder Abteilungen blockiert oder zugelassen werden. Je nach beabsichtigter Funktion kann der Zugang des Codes zum Unternehmensnetz zugelassen oder abgewiesen werden. Mit SurfinGate können Administratoren mobilen Code aktivieren und unternehmensweite Sicherheitsrichtlinien für ActiveX-Code, Java-Code, JavaScript-Code, Visual Basic Script, Plug-Ins und Cookies verwalten, steuern und erzwingen.

SurfinGate beinhaltet die folgenden Komponenten:

- SurfinGate-Server
- SurfinConsole
- SurfinGate-Datenbank
- Plug-In für WTE-Integration

Der SurfinGate-Server agiert als HTTP-Proxy-Server oder als Service für die Firewall oder den Proxy. Der SurfinGate-Server kann hinter der Unternehmens-Firewall und beliebigen anderen vorhandenen Proxies plaziert werden und agiert auch als HTTP-Server. Durch diese Architektur ist es möglich, Datenverkehr mit mobilem Code zu stoppen und zu überprüfen, bevor er Schaden anrichten kann.

Ein Netzadministrator benutzt die SurfinConsole, um im Unternehmen zentrale Sicherheitsrichtlinien für mobilen Code zu verwalten und festzulegen. Die SurfinConsole kann mehrere SurfinGate-Server im Netz steuern und auf der Basis von Benutzern oder Gruppen oder über angepaßte Listen von akzeptablem oder nicht akzeptablem Code Regeln für mobilen Code innerhalb des Unternehmens durchsetzen.

Die SurfinGate-Datenbank speichert Details von Sicherheitsprofilen für Minianwendungen (Applet Security Profiles, ASPs) einschließlich der Informationen über Benutzer und Gruppen und der für sie geltenden Sicherheitsrichtlinien. Da SurfinGate den Inhalt des gesamten mobilen Codes dynamisch untersucht, ist die Datenbank für die Sicherheit nicht erforderlich, sie verbessert jedoch die Leistung bei umfangreichen Operationen.

Anmerkung: Möglicherweise enthält die SurfinGate-Dokumentation Informationen über die Kontaktaufnahme mit Finjan, wenn Service und Unterstützung benötigt werden. Wird SurfinGate für Windows NT jedoch als Teil des Angebots SecureWay FirstSecure oder SecureWay Boundary Server geliefert, muß Kontakt mit IBM aufgenommen werden, wenn Service und Unterstützung benötigt werden.

Kapitel 7. Intrusion Immunity im Netz planen

Bei den bis jetzt beschriebenen Sicherheitstechnologien stand der Schutz gegen Sicherheitsrisiken im Vordergrund. Ein ebenso wichtiger Sicherheitsaspekt ist jedoch das Erkennen von Gefahrenquellen. Die Intrusion Immunity-Produkte in FirstSecure bieten das Erkennen von Attacken auf das System und Antivirenschutz, damit Gefahrenquellen für die Systemsicherheit erkannt werden können.

Antivirus-Software bietet Schutz gegen alle Arten von heimtückischem Code wie Trojanische Pferde, Makroviren, destruktive ActiveX-Steuerungen und destruktive Java-Minianwendungen. Der Virenschutz ist ein wesentlicher Bestandteil aller Sicherheitslösungen. Die FirstSecure-Antivirusprodukte erfüllen die folgenden wichtigen Anforderungen, die an Antivirusprodukte gestellt werden:

- Abdeckung einer Vielzahl von Clients, damit eine benutzerfreundliche und konsistente Methode hinsichtlich des Virenschutzes sowohl bei stationären als auch bei mobilen Clients besteht.
- Teilnehmerberechtigungseintrag für Viruskennungen. Die regelmäßige Aktualisierung von Viruskennungen ist entscheidend für die Aufrechterhaltung eines wirksamen Schutzes gegen die neuesten Formen von Viren.
- Verteilung der Antivirus-Aktualisierungen von Servern auf Clients auf der Basis der Sicherheitsrichtlinien im Unternehmen, damit die Antivirusrichtlinien wirksam umgesetzt werden können.

Einsatz von Tivoli Cross-Site for Security

Tivoli Cross-Site for Security schützt Systeme, die anfällig für feindliche Attacken sein können, durch das netzgestützte Erkennen von Attacken. Sie können Tivoli Cross-Site for Security-Agents überall dort einsetzen, wo eine Verwaltungsdomäne mit dem Internet verbunden wird. Tivoli Cross-Site for Security überwacht Netze, um interne und externe Attacken zu erkennen, und bietet folgende Vorteile:

- Erkennen von Attacken auf die Systemsicherheit in Echtzeit und Mitteilung über mögliche Attacken an den Cross-Site for Security-Administrator.
- Konfigurierbare Richtlinien, mit denen unterschiedliche Richtlinien für Agents in der DMZ und Agents im Intranet festgelegt werden können.
- Online-Änderung von Sicherheits-Agent-Richtlinien, damit schnell auf geänderte Umgebungsbedingungen reagiert werden kann.

- Integration mit den Tivoli-Enterprise-Anwendungen, damit das Tivoli-Verwaltungssystem im Unternehmen verbessert werden kann.

Tivoli Cross-Site for Security kann folgendes:

- Das Suchen von Eindringlingen nach Sicherheitslücken und das Überschwemmen mit E-Mail erkennen.
- IP-Datenverkehr überwachen
- Anschlußservices überwachen
- DNS-, Mount-Service und Netzdateisystemanforderungen erkennen und beantworten
- Speicherauszüge von Port Mapper-Serviceanforderungen und -antworten erkennen.
- RStatd-Aufrufe erkennen
- Anforderungen für bestimmte Maskennamen und Dateinamen erkennen
- SMB-gestützte Attacken auf PC-Datei-Server erkennen
- Internet Control Message Protocol erkennen

Mit Cross-Site for Security können Sie den Netzdatenverkehr überwachen und Attacken auf das System erkennen. Cross-Site for Security überwacht den Datenverkehr sowohl in der DMZ, die Ihr Intranet vom Internet isoliert, als auch auf Ihrem internen Netz.

Cross-Site for Security kann beispielsweise folgende Arten von Attacken auf das System erkennen:

- Verdächtige Kennungen oder Muster
- Überschwemmen mit E-Mail
- Attacken über das Netz
- Windows-Netzattacken
- Attacken über ferne Prozeduren
- Unbefugte Nutzung von Services
- Unbefugter Datenaustausch auf dem Netz
- Verdächtige Aktivitäten

Cross-Site for Security schützt Ihr Netz durch den Cross-Site for Security-Agent und den Cross-Site for Security-Verwaltungs-Server. Wenn ein Agent eine kritische Attacke erkennt, sendet er ein verschlüsseltes Ereignis an den Cross-Site for Security-Verwaltungs-Server, der die Informationen sofort protokolliert und antwortet. Sie können den Cross-Site for Security-Verwaltungs-Server so konfigurieren, daß ein Alert an die Konsole oder eine E-Mail an einen Administrator gesendet oder der Administrator im Bereitschaftsdienst informiert wird.

Tivoli Cross-Site for Security-Lizenzberechtigung erhalten

Zum Aktivieren Ihres Tivoli Cross-Site for Security-Produkts benötigen Sie eine angepaßte Lizenzberechtigung.

Diese Lizenzberechtigung können Sie über die Tivoli Cross-Site-Web-Site abrufen, indem Sie die folgenden Schritte ausführen:

1. Legen Sie den Berechtigungsnachweis (das Dokument *Passport Advantage Proof of Entitlement*), der mit allen FirstSecure-Produkten geliefert wird, die Tivoli Cross-Site for Security-CD-ROM und das Buch *Tivoli Cross-Site for Security Installation* bereit.
2. Suchen Sie die Bestellnummer (eine achtstellige Zahl, die mit einer 5 beginnt) und die Kundennummer (eine siebenstellige Zahl, die mit einer 7 beginnt) auf dem Berechtigungsnachweis (*Passport Advantage Proof of Entitlement*). Sie benutzen diese Nummern für den ersten Zugriff auf die Tivoli Cross-Site-Web-Site.
3. Melden Sie sich an einem Computer mit Internet-Zugang mit einem Web-Browser an der Tivoli Cross-Site-Web-Site an. Die Adresse (URL) der Web-Site ist `www.cross-site.com/support/licensing/`.
4. Geben Sie die Bestellnummer, die Kundennummer und Kontaktinformationen ein. Sie müssen auch den Domänennamen des Servers angeben, auf dem Tivoli Cross-Site for Security installiert werden soll.
5. Folgen Sie den weiteren Anweisungen auf der Web-Site.
6. Haben Sie Probleme beim Zugriff auf die Tivoli Cross-Site-Web-Site für die Lizenzberechtigung, nehmen Sie telefonisch oder per E-Mail unter licensing@cross-site.com mit der Tivoli Cross-Site-Unterstützung Kontakt auf.

Zugehörige Tivoli Cross-Site-Produkte

Die Tivoli Cross-Site-Produktfamilie enthält weitere Komponenten, die nicht Teil der FirstSecure-Produktfamilie sind:

- Tivoli Cross-Site for Availability überwacht und berichtet, in welchem Umfang Endbenutzer auf Ihre Web-Site zugreifen können.
- Tivoli Cross-Site for Deployment dehnt die Reichweite Ihres Unternehmens aus und ermöglicht das Verteilen und Verwalten kritischer Anwendungen und Informationen über das Internet.

Diese Produkte können in der Tivoli Cross-Site for Security-Dokumentation aufgeführt sein, sie müssen jedoch separat gekauft werden.

Datenverkehr mit Tivoli Cross-Site for Security überwachen

Der Cross-Site for Security-Agent ist ein intelligenter "Schnüffler" im Netz. Er überwacht die Pakete im Netz permanent. Der Cross-Site for Security-Agent filtert diese Pakete und sucht nach verschiedenen Kennungen, die verdächtige Aktivitäten darstellen. Diese Kennungen können Anzeichen für Attacken auf dem Netz sein. Der Cross-Site for Security-Agent läuft als *Dämon* unter UNIX und als NT-Dienst unter Windows NT. Das Produkt Cross-Site for Security wird beim Starten des Systems automatisch gestartet. Es bleibt unabhängig davon, ob ein Benutzer angemeldet ist, resident und läuft im Hintergrund.

Wenn eine potentielle Attacke festgestellt wird, ermittelt der Agent den Grad der Bedrohung und legt fest, ob der Verwaltungs-Server sofort informiert oder der Alert in einer lokalen Datei protokolliert wird. Protokolle werden regelmäßig auf den Verwaltungs-Server geladen.

Der Agent nimmt zudem regelmäßig Kontakt mit dem Cross-Site for Security-Verwaltungs-Server auf, um ihm mitzuteilen, daß er noch aktiv ist. Diese Art der Kommunikation wird *Überwachungssignal* (Heartbeat) genannt. Sie können die Intervalle der Überwachungssignale konfigurieren.

Wenn der Verwaltungs-Server ein Überwachungssignal vom Agent erhält, informiert der Verwaltungs-Server den Agent über alle aktualisierten Konfigurationsinformationen, neue Kennungen und Hochladepläne. Der Agent lädt diese Aktualisierungen automatisch herunter und installiert sie.

Tivoli Cross-Site for Security in Ihrem Netz

Sie können Cross-Site for Security so konfigurieren, daß Cross-Site for Security an Ihre Geschäftsanforderungen angepaßt wird. Es müssen die folgenden wichtigen Entscheidungen getroffen werden:

- Wo wird der Cross-Site for Security-Verwaltungs-Server installiert?
- Wie viele Cross-Site for Security-Agents werden benötigt?
- Wo werden die Cross-Site for Security-Agents installiert?

Diese Überlegungen sind neben der Größe, der Topologie und der Bandbreite des Netzes und dem Volumen des Datenverkehrs wichtige Punkte beim Ermitteln der Anzahl der Verwaltungs-Server und -Agents. Überlegungen hinsichtlich der Installation von Tivoli Cross-Site for Security stehen in „Intrusion Immunity - Hardware- und Softwarevoraussetzungen“ auf Seite 71.

Anmerkung: Möglicherweise ist in der Tivoli Cross-Site for Security-Dokumentation beschrieben, mit wem Kontakt aufgenommen werden muß, wenn Service und Unterstützung benötigt werden. Wird Tivoli Cross-Site for Security als Teil des Angebots SecureWay FirstSecure geliefert, muß Kontakt mit IBM aufgenommen werden, wenn Service und Unterstützung benötigt werden.

Einsatz von Norton AntiVirus

Norton AntiVirus, ein Produkt der Symantec Corporation, ist eines der weltweit führenden Antivirusprodukte. Norton AntiVirus kann

- infizierte Dateien isolieren.
- gegen Viren und heimtückische ActiveX-Steuerungen und Java-Minianwendungen schützen.
- gegen Viren schützen, die über E-Mail-Anlagen, heruntergeladene Internet-Dateien, Disketten, Software-CDs oder ein Netz eindringen können.

Norton AntiVirus kann permanent im Hintergrund laufen und schützt so den Computer. Das Symantec-Labor erhöht die Anzahl der Viren, die Norton AntiVirus erkennen kann, permanent. Über die LiveUpdate-Funktion können Sie einmal pro Woche die neuesten Antivirusdefinitionen automatisch von Symantec abrufen.

Durch die Norton AntiVirus-Funktion zum Isolieren von infizierten oder verdächtigen Dateien wird eine solche Datei an einer sicheren Stelle des Computers von anderen Dateien isoliert, um die Verbreitung des Virus zu verhindern, während die Datei korrigiert wird.

Über den Scan-and-Deliver-Assistenten können verdächtige Dateien zwecks Auswertung an Symantec gesendet werden. Das Symantec AntiVirus Research Center (SARC) hilft bei der Lösung des Problems.

Das Norton AntiVirus-Suchprogramm *Bloodhound* läuft im Hintergrund und überwacht das Verhalten von Anwendungen, bei denen die Gefahr einer Infektion durch neue Viren besteht, und teilt diese Anwendungen in Kategorien ein. Verhält sich eine Anwendung wie ein Virus und versucht, andere Programme zu infizieren, kann Bloodhound das Programm stoppen und so eine Infektion anderer Dateien verhindern, bis die neuesten Aktualisierungen der Virusdefinitionen heruntergeladen wurden.

Zu den Norton AntiVirus Solution Release 3.04-Produkten in FirstSecure gehören:

- Desktop-Lösungen:
  - Norton AntiVirus 4.08 für DOS
  - Norton AntiVirus 4.08 für Windows 3.51
  - Norton AntiVirus 5.02 für Windows 95/98
  - Norton AntiVirus 4.08 für Windows NT 3.51
  - Norton AntiVirus 5.02 für Windows NT 4.0
  - Norton AntiVirus 5.03 für Macintosh
  - Norton AntiVirus 5.02 für OS/2

- Server-Lösungen:
  - Norton AntiVirus 4.08 für Windows NT 3.51
  - Norton AntiVirus 5.02 für Windows NT 4.0
  - Norton AntiVirus 4.04 für NetWare
  - Norton AntiVirus 2.0 für Lotus Notes und OS/2
  - Norton AntiVirus 1.52 für Microsoft Exchange
- Gateway-Lösungen:
  - Norton AntiVirus 1.02A für Internet E-Mail-Gateways für NT
  - Norton AntiVirus 1.04 für Firewalls
- Verwaltung:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 für Macintosh Administrator
  - Norton AntiVirus Plus 5.0 für Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 für Tivoli IT Director
  - Weitere Verwaltungs-Tools wie Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Weitere Informationen über Norton AntiVirus stehen in der Datei contents.txt, die sich im Stammverzeichnis der Norton AntiVirus-CD befindet.

Anmerkung: Möglicherweise enthält die Norton AntiVirus-Dokumentation Informationen über die Kontaktaufnahme mit Symantec, wenn Service und Unterstützung benötigt werden. Wird Norton AntiVirus Solution Release 3.04 jedoch als Teil des Angebots SecureWay FirstSecure geliefert, muß Kontakt mit IBM aufgenommen werden, wenn Service und Unterstützung benötigt werden.

Die genauen Installationsschritte stehen in den mit den einzelnen Produkten gelieferten Dokumentationen. Informationen über die Hardware- und Softwarevoraussetzungen enthält Kapitel 13, „Intrusion Immunity - Voraussetzungen und Überlegungen zur Installation“ auf Seite 71.

Kapitel 8. Public Key Infrastructure im Netz planen

Die Public Key Infrastructure-Komponente Trust Authority bietet Internet-Anwendungen die Mittel zur Authentifizierung von Benutzern und zur Gewährleistung einer sicheren Kommunikation. Ein Trust Authority-System baut auf den PKI-Standards (PKI = Public Key Infrastructure) für die Verschlüsselung und Interoperabilität auf und bietet die Infrastruktur, die zum Ausgeben, Veröffentlichen und Verwalten von digitalen Zertifikaten erforderlich ist. Trust Authority beinhaltet folgendes:

- Unterstützung für die Server-Plattformen IBM AIX und Microsoft Windows NT.
- Eine Registrierungsstelle (Registration Authority, RA), die die zur Benutzerregistrierung gehörenden Verwaltungsaufgaben ausführt. Diese Verwaltung, die von automatisierten Prozessen oder von Personen vorgenommen werden kann, beinhaltet die folgenden Arten von Aufgaben:
  - — Bestätigung der Identität eines Benutzers.
  - — Bestätigung oder Zurückweisung von Anforderungen zum Ausstellen, Erneuern oder Widerrufen von Zertifikaten.
  - — Überprüfung, ob der Benutzer über den persönlichen Schlüssel verfügt, der dem allgemeinen Schlüssel in einem Zertifikat zugeordnet ist.
  - — Einhaltung der Regeln in einem bestimmten Geschäftsprozeß oder Zertifikatprofil, damit für bestimmte Arten von Benutzern bestimmte Arten von Zertifikaten ausgegeben werden können.

  Die Registrierungsstelle veröffentlicht zudem Informationen über Zertifikate in einem integrierten Verzeichnis für allgemeine Schlüssel, dem IBM SecureWay Directory (LDAP).
- Eine Zertifizierungsstelle. Die Zertifizierungsstelle
  - — gibt digitale Zertifikate aus und generiert Paare von digitalen Schlüsseln, mit denen die Zertifikate authentifiziert werden können.
  - — unterstützt die gesamte Lebensdauer von Zertifikaten von der Erstregistrierung über die Erneuerung bis zum Widerruf.
  - — Die Registrierungsstelle aktualisiert das Verzeichnis sofort, wenn ein Zertifikat widerrufen wird.
  - — kann Verschlüsselungshardware (beispielsweise den IBM SecureWay 4758 PCI Cryptographic Coprocessor und Smart Cards) verwenden, um die Schlüssel besser schützen zu können.

- Credential Central, eine web-gestützte Registrierungsschnittstelle, die den Erhalt von Browser-Zertifikaten, Server-Zertifikaten und Zertifikaten für bestimmte Einheiten wie Smart Cards erleichtert. Administratoren können diese Registrierungsformulare zudem für die Vorabregistrierung von Endbenutzern für ein PKIX-Zertifikat benutzen.
- Trust Authority-Client, eine eigenständige Windows-Schnittstelle, mit der Benutzer PKIX-Zertifikate ohne einen Web-Browser erhalten, erneuern oder widerrufen können.
- RA Desktop, eine web-gestützte Verwaltungsschnittstelle, über die eine Person als Administrator Anforderungen zum Ausstellen, Erneuern oder Widerrufen von Zertifikaten bestätigen oder zurückweisen kann.
- Ein Protokollierungssubsystem, das Nachrichtenauthentifizierungscodes (Message Authentication Codes, MACs) benutzt, um sicherzustellen, daß von der Trust Authority-Registrierungsstelle oder -Zertifizierungsstelle zugestellte Ereignisse authentifiziert werden können. Über eine konfigurierbare Option kann zudem die Integrität von Protokolleinträgen bei der Protokollierung geschützt werden.
- Mehrere Verwaltungsschnittstellen für das Konfigurieren des Systems, das Ändern von Kennwörtern, übergreifende Zertifizierungsstellen, Prüfprotokolle zur Integritätsprüfung und das gesicherte Starten und Stoppen von Systemkomponenten.
- Eine Anwendungsprogrammierschnittstelle, mit der Anwendungsentwickler angepaßte PKI-Anwendungen schreiben können.
- Integrierte Laufzeitunterstützung für die IBM DB2 Universal Database. Für das IBM SecureWay Directory und die Registrierungsstelle, die Zertifizierungsstelle und die Protokollierungskomponente sind separate Datenbanken vorhanden.

Einsatz von Trust Authority

Das Buch *IBM SecureWay Trust Authority Einführung* enthält genaue Informationen über die Planung und Installation. Dieses Buch enthält Szenarien und Schritte für die Installation unter Windows NT-Servern und AIX.

Kapitel 9. SecureWay Toolbox im Unternehmen planen

Planen Sie die Installation von FirstSecure Toolbox so, daß die Installation in einer Entwicklungsumgebung und nicht im Netz erfolgt. Testen Sie die Anwendungen innerhalb der Entwicklungsumgebung, bevor Sie sie externen Benutzern zur Verfügung stellen.

Berechtigungsservices

Über Berechtigungsservices können Sie überwachen, wer die Berechtigung zum Zugriff auf Ihre Web-Site hat. Die Authentifizierung erfolgt auf der Basis von Kennwörtern oder allgemeinen Schlüsseln. Durch diese Maßnahmen wird die Integrität und Vertraulichkeit der Daten auf Ihrer Site geschützt. Berechtigungsservices erstellen Zugriffssteuerungslisten (ACLs), in denen definiert ist, wer auf Objekte Ihrer Site zugreifen darf und wie dieser Zugriff erfolgen darf. Berechtigungsservices ermöglichen zudem das Definieren geschützter Objekte und das Erstellen von Kennwörtern für die einstufige Anmeldung. Zwecks Vereinfachung der Verwaltung von Sicherheitsrichtlinien werden diese Sicherheits-Tools zentral verwaltet. Berechtigungsservices werden von den Berechtigungs-APIs des IBM SecureWay Policy Director unterstützt.

Services für Zertifizierungsstellen

Services für Zertifizierungsstellen werden von X.509 Public Key Infrastructure for Multiplatforms und dem IBM KeyWorks Toolkit unterstützt.

Durch Services für Zertifizierungsstellen können Sie die Sicherheit durch die Verwaltung digitaler Zertifikate gewährleisten. Diese Services beinhalten APIs für die gesamte Lebensdauer dieser Zertifikate von der Ausstellung über die Erneuerung bis zum Widerruf. Zudem können sie zum Veröffentlichen von Listen mit widerrufenen Zertifikaten benutzt werden. Die APIs benutzen die Verschlüsselung über allgemeine Schlüssel und Smart Cards als Mittel zur Authentifizierung der Benutzer von Zertifikaten.

X.509 Public Key Infrastructure for Multiplatforms, auch als PKIX bezeichnet, wird über PKIX-APIs geliefert. Diese APIs ermöglichen das Erstellen, Verwalten, Speichern, Verteilen und Widerrufen von Zertifikaten über die Anwendung für End-Definitionseinheiten (End Entity, EE), die Zertifizierungsstelle (Certificate Authority, CA) und die Registrierungsstelle (Registration Authority, RA). Die APIs verfügen über eine Schnittstelle zu IBM SecureWay Trust Authority und basieren auf IBM KeyWorks.

Informationen über die PKIX-APIs enthält das Buch *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*. Weitere Informationen über IBM KeyWorks enthalten die Veröffentlichungen in der Liste der mit der Toolbox gelieferten Dokumentationen in Kapitel 16, „Mit FirstSecure gelieferte Dokumentationen“ auf Seite 91.

Verzeichnisservices

Verzeichnisservices werden über den IBM SecureWay Directory-Client unterstützt.

Verzeichnisservices benutzen das Lightweight Directory Access Protocol (LDAP), um Verzeichnisse zu verwalten und zu steuern und um auf Verzeichnisse zuzugreifen. Diese Services basieren auf einem Client/Server-Modell, das den Client-Zugriff auf einen LDAP-Server ermöglicht. Verzeichnisservices bieten eine Möglichkeit zum Verwalten von Verzeichnisinformationen an einem zentralen Standort (Speichern, Aktualisieren, Abrufen und Datenaustausch). Verzeichnisservices benutzen Secure Sockets Layer (SSL) zum Verschlüsseln von Informationen.

Weitere Informationen über Verzeichnisservices enthalten die Veröffentlichungen in der Liste der mit der Toolbox gelieferten IBM SecureWay Directory Client-Dokumentationen in Kapitel 16, „Mit FirstSecure gelieferte Dokumentationen“ auf Seite 91.

KeyWorks-Services für Verschlüsselungs- und Authentifizierungsverwaltung

Services für Verschlüsselungs- und Authentifizierungsverwaltung werden von IBM KeyWorks Toolkit (auch als KeyWorks bezeichnet) unterstützt.

Die KeyWorks-Services für Verschlüsselungs- und Authentifizierungsverwaltung verschlüsseln und entschlüsseln Informationen zur Steuerung des Zugriffs auf die Informationen. Diese Services erstellen und überprüfen digitale Unterschriften, um die Identität von Personen und Computern im Netz zu authentifizieren. In IBM Key Recovery Service Provider ist ein Schlüsselwiederherstellungssystem integriert, das die Wiederherstellung von verschlüsselten Informationen ermöglicht, ohne daß der Schlüssel verteilt wird.

KeyWorks ist ein Toolkit für Verschlüsselungs- und Authentifizierungsservices. KeyWorks besteht aus einer Gruppe von geschichteten Sicherheitsservices und zugeordneten Programmierschnittstellen, die eine integrierte Gruppe von Sicherheitsfunktionen für Informationen und Übertragungen liefern.

Jede Schicht baut auf den eher grundlegenden Services der direkt unter ihr befindlichen Schicht auf. Diese Schichten beginnen mit grundlegenden Elementen wie Verschlüsselungsalgorithmen, Zufallszahlen und eindeutigen Kennungen in den unteren Schichten und setzen sich bis zu digitalen Zertifikaten, Mechanismen zur Verwaltung und Wiederherstellung von Schlüsseln und Protokollen für gesicherte Transaktionen in den höheren Schichten fort.

KeyWorks unterstützt Landessprachen, das Produkt ist daher nicht abhängig von bestimmten Sprachen und Zeichensätzen.

Weitere Informationen über die KeyWorks-C-APIs enthalten die Veröffentlichungen in der Liste der mit der Toolbox gelieferten KeyWorks-Dokumentationen in Kapitel 16, „Mit FirstSecure gelieferte Dokumentationen“ auf Seite 91.

SSL-Protokollservices

Secure Sockets Layer-Protokollservices werden von dem IBM Secure Sockets Layer (SSL) Toolkit unterstützt.

Mit den SSL-Protokollservices können Sie entscheiden, wer Zugriff auf Ihre Daten hat. Diese Services verschlüsseln Daten über allgemeine und persönliche Schlüssel beispielsweise zwecks Benutzerauthentifizierung, Verhinderung des Zugriffs durch unbefugte Clients und Verhinderung von Datenfälschungen. Sie können steuern, wem Sie Zertifikate ausstellen, daher können Sie die Sicherheit beim Zugriff auf Ihre Daten selbst steuern.

Die SSL-Technologie ist in mehrere weitere APIs zum Verschlüsseln von Daten und Erstellen von Kennwörtern integriert.

Teil 3. Voraussetzungen für die Installation und Integration

Dieser Teil enthält Informationen über die Voraussetzungen für die Installation und Integration der einzelnen Komponenten. Es werden die Hardware- und Softwarevoraussetzungen für die einzelnen Produkte und alle erforderlichen Anwendungen oder Datenbankprodukte aufgeführt.

Kapitel 10. Installation von FirstSecure planen

Vor der Installation der FirstSecure-Komponenten müssen die folgenden Abschnitte gelesen werden, damit die Verfügbarkeit der erforderlichen Hardware und Software gewährleistet ist. Informationen über die neuesten Aktualisierungen an FirstSecure sind im Internet unter

www.ibm.com/software/security/firstsecure

verfügbar. Rufen Sie vor der Installation der Produkte die Web-Site auf, um zu überprüfen, ob neueste Aktualisierungen vorliegen.

Genaue Anweisungen zur Installation und Konfiguration der FirstSecure-Komponenten enthält die mit den einzelnen Komponenten gelieferte Literatur.

Allgemeine Systemvoraussetzungen

In diesem Abschnitt werden die allgemeinen Systemvoraussetzungen für die FirstSecure-Produkte beschrieben. Spezielle Hardware- und Softwarevoraussetzungen für die einzelnen Komponenten stehen in den entsprechenden Kapiteln.

Zur Installation der FirstSecure-Komponenten ist Hardware erforderlich, auf der eines der folgenden Server-Betriebssysteme laufen kann:

- Microsoft Windows NT Version 4 mit Service Pack 5.
- AIX Version 4.3.1 oder höher.
- Sun Solaris Version 2.6 oder höher.

  Anmerkung: Für die Toolbox ist unter Solaris Sun Solaris Version 2.6 mit dem Fix Pack vom Mai 1999 erforderlich.

Jede der FirstSecure-Komponenten läuft auf mindestens einem der oben aufgeführten Betriebssysteme. In den Kapiteln über die einzelnen Komponenten sind die unterstützten Betriebssystemplattformen und andere Softwarevoraussetzungen für die einzelnen Komponenten aufgeführt. Innerhalb dieser Betriebssysteme werden Server, Verwaltungskonsolen und Client-Systeme benötigt. Die folgenden Abschnitte enthalten eine Übersicht über diese Voraussetzungen.

Betriebssystemvoraussetzungen für Server und Clients

Informationen über die Betriebssystemvoraussetzungen für SecureWay-Produkte enthält Tabelle 1.

Tabelle 1. Betriebssystemvoraussetzungen für Server und Clients

Betriebssystem	**Mindest-Release-Stand des Servers**	**Mindest-Release-Stand des Clients**
Windows NT	Version 4.0, Service Pack 5	Version 4.0, Service Pack 5
IBM AIX	Version 4.3.1	Version 4.3.1
Sun Solaris	Version 2.6	Version 2.6
Windows 95	-	Alle Versionen werden unterstützt
Windows 98	-	Alle Versionen werden unterstützt
Windows 3.1 (nur Norton AntiVirus)	-	Alle Versionen werden unterstützt
IBM OS/2 (nur Norton AntiVirus)	-	Version 4.0, FixPak 6 oder höher

Einzelheiten und Voraussetzungen für Komponenten

In den folgenden Kapiteln sind die Hardware- und Softwarevoraussetzungen für die FirstSecure-Komponenten aufgeführt. In den folgenden Kapiteln werden die Module genau beschrieben und die Hardware- und Softwarevoraussetzungen für die einzelnen Module aufgeführt. Die Kapitel enthalten zudem eine Übersicht über die Installation und Konfiguration der einzelnen Produkte einschließlich der Überlegungen hinsichtlich der Integration mit anderen Komponenten.

- Kapitel 11, „Policy Director - Voraussetzungen und Überlegungen zur Installation“ auf Seite 61
- Kapitel 12, „SecureWay Boundary Server - Voraussetzungen und Überlegungen zur Installation“ auf Seite 63
- Kapitel 13, „Intrusion Immunity - Voraussetzungen und Überlegungen zur Installation“ auf Seite 71
- Kapitel 14, „Public Key Infrastructure - Voraussetzungen und Überlegungen zur Installation“ auf Seite 79
- Kapitel 15, „Toolbox - Voraussetzungen und Überlegungen zur Installation“ auf Seite 85

Kapitel 11. Policy Director - Voraussetzungen und Überlegungen zur Installation

In diesem Kapitel werden die Hardware- und Softwarevoraussetzungen für den Policy Director aufgeführt. Es enthält zudem die für die Integration mit anderen FirstSecure-Produkten erforderlichen Installationsvoraussetzungen.

Policy Director - Hardware- und Softwarevoraussetzungen

In Tabelle 2 sind die Hardwarevoraussetzungen für den Policy Director aufgeführt.

Tabelle 2. Hardwarevoraussetzungen für den Policy Director

Plattform	Mindestplattenspeicherplatz	Mindesthauptspeicher
Windows NT-Server: Intel oder Intel-kompatibler 80486 mit 133 MHZ oder höher	16 MB	64 MB
AIX-Server: Hardware mit AIX 4.3.1	16 MB	64 MB
Solaris-Server: Hardware mit Solaris 2.6	16 MB	64 MB

Für die Policy Director-Komponenten bestehen folgende Softwarevoraussetzungen:

Policy Director-Server

- Windows NT-Server Version 4.0, Service Pack 5
- AIX Version 4.3.1
- Sun Solaris, Version 2.6

NetSEAT-Clients

- Windows NT-Server Version 4.0, Service Pack 5
- Windows 95
- Windows 98

Verwaltungskonsole (Management Console)

- Windows NT Workstation
- Windows NT Server-Client
- AIX Version 4.3.1-Client
- Sun Solaris, Version 2.6-Client

Für den Policy Director ist weitere Software erforderlich, die in dem Paket enthalten ist. Gehen Sie zur Installation der für den Policy Director erforderlichen Software anhand der Anweisungen im Buch *IBM SecureWay Policy Director Installation und Konfiguration* vor.

Policy Director - Installationsvoraussetzungen

Unter www.ibm.com/software/security/policy sind alle Aktualisierungen an den aktuellen Softwarevorbedingungen für den Policy Director aufgeführt.

Integration von Policy Director und Trust Authority

IBM SecureWay Trust Authority bietet Authentifizierung, indem jeder Benutzer auf seine Identität überprüft wird. Trust Authority gibt anhand der Informationen im IBM SecureWay Directory (auch Lightweight Directory Access Protocol oder LDAP genannt) Zertifikate an Benutzer aus.

Der Policy Director wiederum benutzt diese Zertifikate, um den einzelnen Benutzern die Berechtigung ausschließlich für die erlaubten Ressourcen zu erteilen. Der Policy Director speichert seine Informationen in demselben IBM SecureWay Directory.

Ihr e-business kann eine einzelne Benutzerdefinition mit allen Policy Director-Berechtigungen und allen Trust Authority-Informationen haben. Wenn Sie auch SecureWay Boundary Server-Informationen im IBM SecureWay Directory speichern, kann der Policy Director auch diese Verwaltung für Sie übernehmen.

Kapitel 12. SecureWay Boundary Server - Voraussetzungen und Überlegungen zur Installation

In diesem Kapitel werden die Hardware- und Softwarevoraussetzungen für den SecureWay Boundary Server aufgeführt. Es enthält zudem die für die Integration mit anderen SecureWay Boundary Server-Produkten erforderlichen Installationsvoraussetzungen.

SecureWay Boundary Server - Hardware- und Softwarevoraussetzungen

Die Hardwarevoraussetzungen für die SecureWay Boundary Server-Komponenten sind in Tabelle 3 und Tabelle 4 auf Seite 65 aufgeführt.

Tabelle 3 (Seite 1 von 2). Hardwarevoraussetzungen für SecureWay Boundary Server-Komponenten

SecureWay Boundary Server-Komponente	**Maschinentyp**	**Plattenspeicherplatz**	**Hauptspeicher**	**Weitere Voraussetzungen**
IBM SecureWay Firewall[1]	NT: Pentium® mit 133 MHz oder höher AIX: RS/6000-Maschine, die AIX 4.3.2 unterstützt	NT: 24 MB[2] AIX: 307 MB	NT: 64 MB AIX: 64 MB	2 Netzschnittstellenkarten
ACE/Server	NT: Pentium mit 166 MHz oder höher (nur Einzelprozessoren) AIX: Maschine, die AIX 4.2 unterstützt	Software für primären Server: 50 MB Ausweich-Server: 22 MB Benutzerdatenbank (anfänglich): 4 MB Installation: 240 MB	Minimum: 32 MB	Der tatsächliche Speicherbedarf hängt von der Anzahl der Benutzer ab.

Tabelle 3 (Seite 2 von 2). Hardwarevoraussetzungen für SecureWay Boundary Server-Komponenten

SecureWay Boundary Server-Komponente	Maschinentyp	Plattenspeicherplatz	Hauptspeicher	Weitere Voraussetzungen
SurfinGate				
Server	Pentium mit 233 MHz oder höher	20 MB	Minimum: 128 MB Empfohlen: 256 MB	
Console	Pentium mit 233 MHz oder höher	15 MB	Minimum: 32 MB Empfohlen: 64 MB	
MIMEsweeper für IBM SecureWay Release 2				
MAILsweeper	Pentium mit 200 MHz oder höher	1 GB	64 MB	1 Netzschnittstellenkarte
WEBsweeper	Pentium mit 400 MHz oder höher	1 GB	128 MB + 1 MB pro gleichzeitige Web-Verbindung	1 Netzschnittstellenkarte

Anmerkungen:

1. Weitere Informationen enthält die mit IBM Firewall gelieferte Dokumentation.
2. Zudem sind 138 MB Plattenspeicherplatz für den Netscape-Browser erforderlich.

Tabelle 4 (Seite 1 von 2). Softwarevoraussetzungen für SecureWay Boundary Server-Komponenten

SecureWay Boundary Server-Komponente	Microsoft Windows-Plattformen		AIX	Solaris
	Client	Server	Server	Server
IBM SecureWay Firewall	Windows 95, IPSec-Client	Windows NT Server Version 4.0, Service Pack 5[1]	AIX 4.3.2	Nicht verfügbar
ACE/Server	Windows NT Workstation 4.0, Service Pack 2 oder höher	Windows NT Server Version 4.0, Service Pack 5 oder höher	AIX 4.2	Solaris 2.5.1

Tabelle 4 (Seite 1 von 2). Softwarevoraussetzungen für SecureWay Boundary Server-Komponenten

SecureWay Boundary Server-Komponente	**Microsoft Windows-Plattformen**		**AIX**	**Solaris**
	Client	**Server**	**Server**	**Server**
SurfinGate 4.05				
Server	Nicht verfügbar	Windows NT 4.0[2]	Nicht verfügbar	Nicht verfügbar
Console	Windows NT 4.0 oder höher[2] Windows 95, Windows 98	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
MIMEsweeper für IBM SecureWay Release 2				
MAILsweeper	Nicht verfügbar	Windows NT 4.0[3]	Nicht verfügbar	Nicht verfügbar
WEBsweeper	Windows NT Workstation 4.0, Service Pack 3 oder höher	Windows NT 4.0[4]	Nicht verfügbar	Nicht verfügbar

Anmerkungen:

1. Stellen Sie in der mit IBM Firewall für Windows NT gelieferten Dokumentation fest, welche Korrekturen (Fixes) erforderlich sind.
2. Zudem muß folgendes berücksichtigt werden:
   - Der Windows-Netz-Client für Microsoft Windows ist erforderlich.
   - Windows NT Workstation wird nicht unterstützt.
3. Zudem muß folgendes berücksichtigt werden:
   - NT 3.5.1 und Windows NT Workstation werden nicht unterstützt.
   - Es ist eine der folgenden Umgebungen erforderlich:
     — Microsoft Exchange
     — SMTP
     — cc:Mail™
     — Groupwise
     — Lotus Notes
4. „Überlegungen zu MIMEsweeper“ auf Seite 70 enthält Empfehlungen für MIMEsweeper.

Überlegungen zu den SecureWay Boundary Server-Komponenten

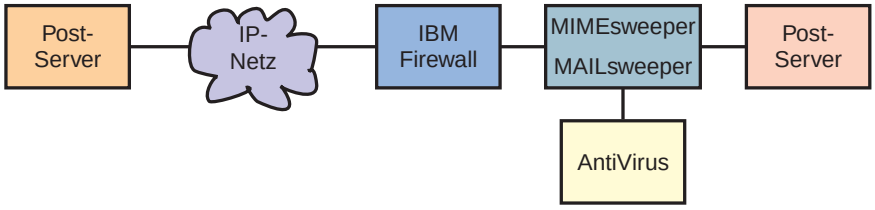
In den folgenden Abschnitten sind die Überlegungen hinsichtlich der Installation und Konfiguration der SecureWay Boundary Server-Komponenten aufgeführt.

Überlegungen zu IBM Firewall

Die Überlegungen zu IBM Firewall beinhalten hauptsächlich, wo IBM Firewall in bezug auf die anderen SecureWay Boundary Server-Produkte im Datenverkehrsstrom installiert werden soll.

Beispielkonfigurationen

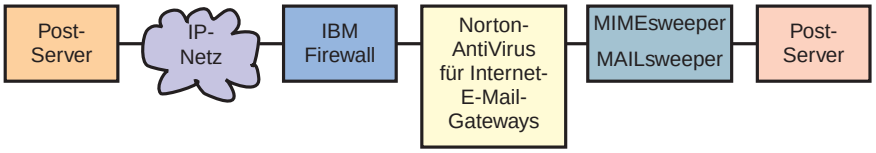
IBM Firewall und MAILsweeper - Beispielkonfiguration: Wird sowohl IBM Firewall als auch MIMEsweeper installiert, kann die in diesem Abschnitt beschriebene Konfiguration benutzt werden.



- MAILsweeper ist der Teil von MIMEsweeper, der den Inhalt von Post überprüft. MAILsweeper verfügt über eine Funktion zur Aktivierung von Antivirusprüfungen.
- MAILsweeper befindet sich zwischen IBM Firewall und den gesicherten SMTP-Servern.
- IBM Firewall zeigt auf MAILsweeper als Post-Host zum Weiterleiten von Post.
  - Damit der Postdatenverkehr fließen kann, müssen für IBM Firewall vordefinierte Regeln für den Postdatenverkehr konfiguriert werden.
- Auch die SMTP-Server müssen auf MAILsweeper als Post-Host zum Weiterleiten von Post zeigen.
- MAILsweeper überprüft den Inhalt sowohl bei ankommender als auch bei abgehender Post.

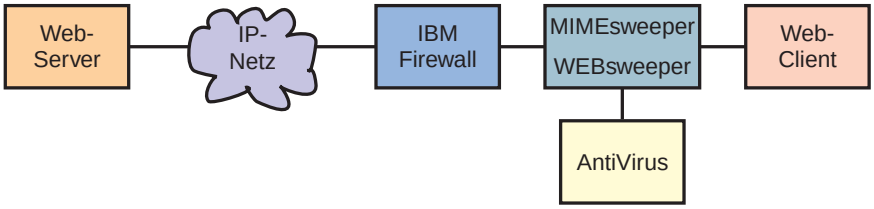
IBM Firewall, Norton AntiVirus für Internet-E-Mail-Gateways und MIMEsweeper - Beispielkonfiguration: Wird IBM Firewall, Norton AntiVirus für Internet-E-Mail-Gateways und MIMEsweeper installiert, kann die in diesem Abschnitt beschriebene Konfiguration benutzt werden.

Bei diesem Szenario werden IBM Firewall, Norton AntiVirus für Internet-E-Mail-Gateways und MAILsweeper in einer Kette kombiniert, um Post auf Viren und Inhalt zu überprüfen (siehe Darstellung in dem folgenden Diagramm).



- Die Firewall zeigt auf Norton AntiVirus für Internet-E-Mail-Gateways als ihren gesicherten Post-Server. Dieser spezielle Datenverkehr ist nur möglich, wenn die korrekten Firewall-Regeln definiert werden.
- Norton AntiVirus für Internet-E-Mail-Gateways zeigt auf MAILsweeper als Weiterleitungsfunktion für gesicherte Post und bei abgehender Post auf die Firewall.
- Wird Post an MAILsweeper weitergeleitet, überprüft MAILsweeper diese weitergeleitete Post und leitet sie dann anhand der Leitwegtabellen oder MX-Satzsuchfunktionen an den korrekten Server weiter. Befinden sich MAILsweeper und Norton AntiVirus für Internet-E-Mail-Gateways auf derselben Maschine, muß der empfangende Anschluß (Port) für MAILsweeper geändert werden, um Konflikte mit Norton AntiVirus für Internet-E-Mail-Gateways zu vermeiden.

IBM Firewall und WEBsweeper - Beispielkonfiguration: Wird sowohl IBM Firewall als auch MIMEsweeper installiert, kann die in diesem Abschnitt beschriebene Konfiguration benutzt werden.



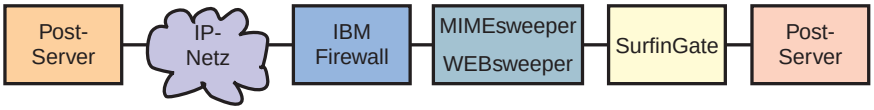
- WEBsweeper ist der Teil von MIMEsweeper, der den Web-Datenverkehr überprüft. WEBsweeper verfügt über eine Funktion zur Aktivierung von Antivirusprüfungen.
- WEBsweeper arbeitet als Zwischen-Proxy. Clients zeigen auf WEBsweeper als ihren Proxy. WEBsweeper wird dann so konfiguriert, daß der Datenverkehr an den Firewall-Proxy weitergeleitet wird.
- Auf der Firewall müssen Regeln definiert werden, damit der Proxy-Datenverkehr möglich wird.

- Proxy-Anforderungen sind nur aus dem gesicherten Netz hinter der Firewall möglich.
- WEBsweeper bearbeitet HTTPS nicht. Soll HTTPS benutzt werden, muß WEBsweeper umgangen werden, um Probleme mit der Firewall zu vermeiden und die Überprüfung des gesamten Web-Datenverkehrs zu gewährleisten. Es muß direkt auf den Firewall-Proxy gezeigt werden. Der Web-Datenverkehr ist zwar immer noch gesichert, aber er wird von WEBsweeper nicht überprüft.

IBM Firewall und SurfinGate - Beispielkonfiguration: Werden IBM Firewall und SurfinGate installiert, kann die in diesem Abschnitt beschriebene Konfiguration benutzt werden.

- SurfinGate überprüft den Web-Datenverkehr auf ActiveX-Steuerungen und andere Elemente.
- SurfinGate agiert als Web-Zwischen-Proxy. Clients zeigen auf SurfinGate als ihren Proxy für HTTP, FTP und HTTPS. SurfinGate leitet die Anforderung dann an den IBM Firewall-Proxy weiter.
- Auf der Firewall müssen Regeln definiert werden, damit der Proxy-Datenverkehr möglich wird.
- Proxy-Anforderungen sind nur aus dem gesicherten Netz hinter der Firewall möglich.

IBM Firewall, MIMEsweeper und SurfinGate - Beispielkonfiguration: Werden IBM Firewall, MIMEsweeper und SurfinGate installiert, kann die in diesem Abschnitt beschriebene Konfiguration benutzt werden.



- SurfinGate überprüft den Web-Datenverkehr auf ActiveX-Steuerungen und andere Elemente und benutzt andere Überprüfungen als die MIMEsweeper-Komponente WEBsweeper.
- SurfinGate und WEBsweeper agieren als Web-Zwischen-Proxies. Clients zeigen auf SurfinGate als ihren Proxy für HTTP und FTP. SurfinGate leitet die Anforderung dann an WEBsweeper weiter. WEBsweeper leitet die Anforderung dann an den IBM Firewall-Proxy weiter.

- Auf der Firewall müssen Regeln definiert werden, damit der Proxy-Datenverkehr möglich wird. Diese Regeln sind im IBM eNetwork Firewall Version 3.3 für Windows NT Benutzerhandbuch definiert.
- Proxy-Anforderungen sind nur aus dem gesicherten Netz hinter der Firewall möglich.
- WEBsweeper bearbeitet HTTPS nicht. Soll HTTPS benutzt werden, muß WEBsweeper umgangen werden, um Probleme mit der Firewall zu vermeiden und die Überprüfung des gesamten Web-Datenverkehrs zu gewährleisten. Es muß direkt auf den Firewall-Proxy gezeigt werden. Der Web-Datenverkehr ist zwar immer noch gesichert, aber er wird von WEBsweeper nicht überprüft.

Überlegungen zu MIMEsweeper

Ein typisches WEBsweeper-System sieht wie folgt aus:

- Intel Pentium mit 400 MHz oder höher.
- 1 GB Plattenspeicherplatz und 128 MB Arbeitsspeicher.
- Windows NT Server oder Workstation Version 4.0-Server mit Service Pack 3 oder höher.
- TCP/IP-Protokoll einschließlich einem Host-Namen und Domänennamen.
- Antivirus-Tools.

Eine typische WEBsweeper-Umgebung mit hoher Auslastung und bis zu 500 gleichzeitig angemeldeten Benutzern sieht wie folgt aus:

- Zwei Prozessoren, Intel Pentium II mit 450 MHz oder höher.
- 3 GB Plattenspeicherplatz und 256 MB Arbeitsspeicher.
- Windows NT Server oder Workstation Version 4.0-Server mit Service Pack 3 oder höher.
- TCP/IP-Protokoll einschließlich einem Host-Namen und Domänennamen.
- Antivirus-Tools.

Unterstützt Ihre Umgebung mehr als 500 gleichzeitig angemeldete Benutzer, werden mehrere WEBsweeper-Server empfohlen.

Kapitel 13. Intrusion Immunity - Voraussetzungen und Überlegungen zur Installation

In diesem Kapitel werden die Hardware- und Softwarevoraussetzungen für die Intrusion Immunity-Komponenten Tivoli Cross-Site for Security und Norton AntiVirus aufgeführt.

Intrusion Immunity - Hardware- und Softwarevoraussetzungen

In dem folgenden Abschnitt werden die Hardware- und Softwarevoraussetzungen für die Intrusion Immunity-Komponenten aufgeführt.

Die Hardware- und Softwarevoraussetzungen für Tivoli Cross-Site for Security sind in Tabelle 5, Tabelle 6 auf Seite 72 und Tabelle 7 auf Seite 72 aufgeführt. Die Hardware- und Softwarevoraussetzungen für die Norton AntiVirus-Komponenten sind in Tabelle 8 auf Seite 73 und Tabelle 9 auf Seite 73 aufgeführt.

Tabelle 5. Hardware- und Softwarevoraussetzungen für Tivoli Cross-Site for Security-Server

Server-Voraussetzungen	
Betriebssystem	• AIX 4.3.2 • Windows NT Version 4.0, Service Pack 5 • Solaris 2.5.1 oder 2.6
Java	JDK 1.1.6 Revision 04 oder höher
Web-Server	Netscape Enterprise Server 3.51
Datenbank	• IBM DB2 Release 5.2 • Oracle 7.3.4 oder 8.0.4 (empfohlen) • Microsoft SQL-Server
Plattenspeicherplatz	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
Hauptspeicher	256 MB
Auslagerungsspeicher	300 MB (400 MB empfohlen)

Anmerkungen:

1. Netscape Enterprise Server 3.51 und 3.6 werden nicht unterstützt.
2. Patch-Code-Voraussetzungen für Solaris stehen in der Installationsdokumentation für Tivoli Cross-Site for Security.

Tabelle 6. Hardware- und Softwarevoraussetzungen für die Tivoli Cross-Site for Security-Verwaltungskonsole

Voraussetzungen für die Verwaltungskonsole	
Betriebssysteme	• Windows 95 • Windows 98 • Windows NT Version 4.0, Service Pack 5 (Maschine mit 166 MHz oder höher wird empfohlen) • Solaris 2.5.1 oder 2.6 auf Sun SPARC
Plattenspeicherplatz	25 MB auf allen Plattformen
Hauptspeicher	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

Tabelle 7. Hardware- und Softwarevoraussetzungen für Tivoli Cross-Site for Security-Agents

Agent-Voraussetzungen	
Betriebssysteme	• Windows NT Version 4.0, Service Pack 5 oder höher • AIX 4.3.2 • Solaris 2.5.1 oder 2.6 auf Sun SPARC
Java	JDK 1.1.6 Revision 04 oder höher auf Solaris (nur für UNIX erforderlich)
Plattenspeicherplatz	• 15 MB unter Windows NT • 10 MB unter AIX • 10 MB unter Solaris
Hauptspeicher	• 32 MB unter Windows NT • 32 MB unter AIX • 20 MB unter Solaris

Anmerkungen:

1. Netscape Enterprise Server 3.51 und 3.6 werden nicht unterstützt.
2. Patch-Code-Voraussetzungen für Solaris stehen in der Installationsdokumentation für Tivoli Cross-Site for Security.

In Tabelle 8 sind die Hardwarevoraussetzungen für Norton AntiVirus aufgeführt.

Tabelle 8. Hardwarevoraussetzungen für Norton AntiVirus

Intrusion Immunity-Komponente	**Maschinentyp**	**Plattenspeicherplatz**	**Hauptspeicher**	**Weitere Voraussetzungen**
Norton AntiVirus	Intel-CPU	24 MB	Minimum: 16 MB Empfohlen: 32 MB	CD-ROM-Laufwerk
Norton AntiVirus für Internet-E-Mail-Gateways	Pentium 133 oder höher	6 MB	32 MB	CD-ROM-Laufwerk 500 MB - 5 GB für effizienten Postbetrieb

Tabelle 9. Softwarevoraussetzungen für Norton AntiVirus

Intrusion Immunity-Komponente	**Microsoft Windows-Plattformen**		**OS/2**
	Client	**Server**	**Client**
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 oder höher

Anmerkungen:

1. Zudem ist eine TCP/IP-Internet-Verbindung für Norton AntiVirus für Internet-E-Mail-Gateways erforderlich.

Norton AntiVirus ist auf AIX und Solaris nicht verfügbar.

Tivoli Cross-Site for Security - Installationsvoraussetzungen

In den folgenden Abbildungen werden typische Anordnungen von Cross-Site for Security-Agents und Cross-Site for Security-Verwaltungs-Server in einem e-business-Netz gezeigt.

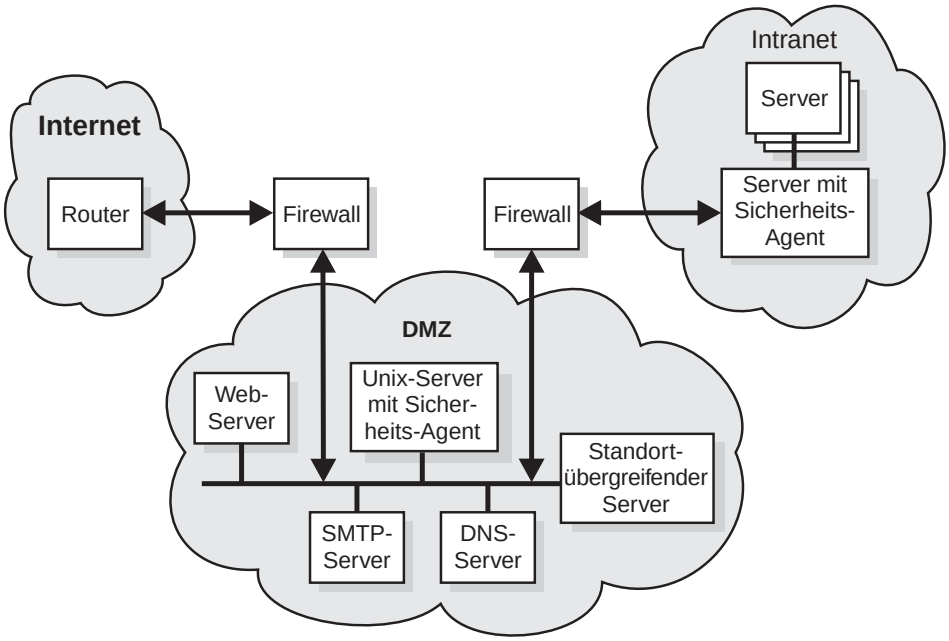


Abbildung 11. Installation des Cross-Site for Security-Verwaltungs-Servers in der DMZ

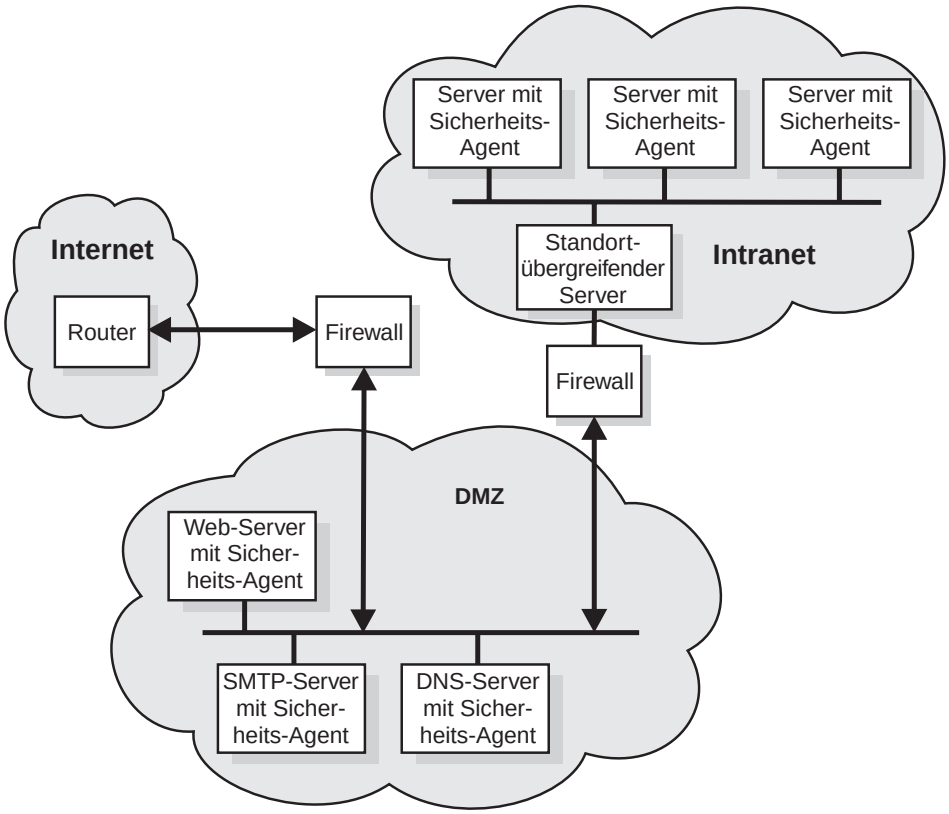


Abbildung 12. Installation des Cross-Site for Security-Verwaltungs-Servers im Intranet

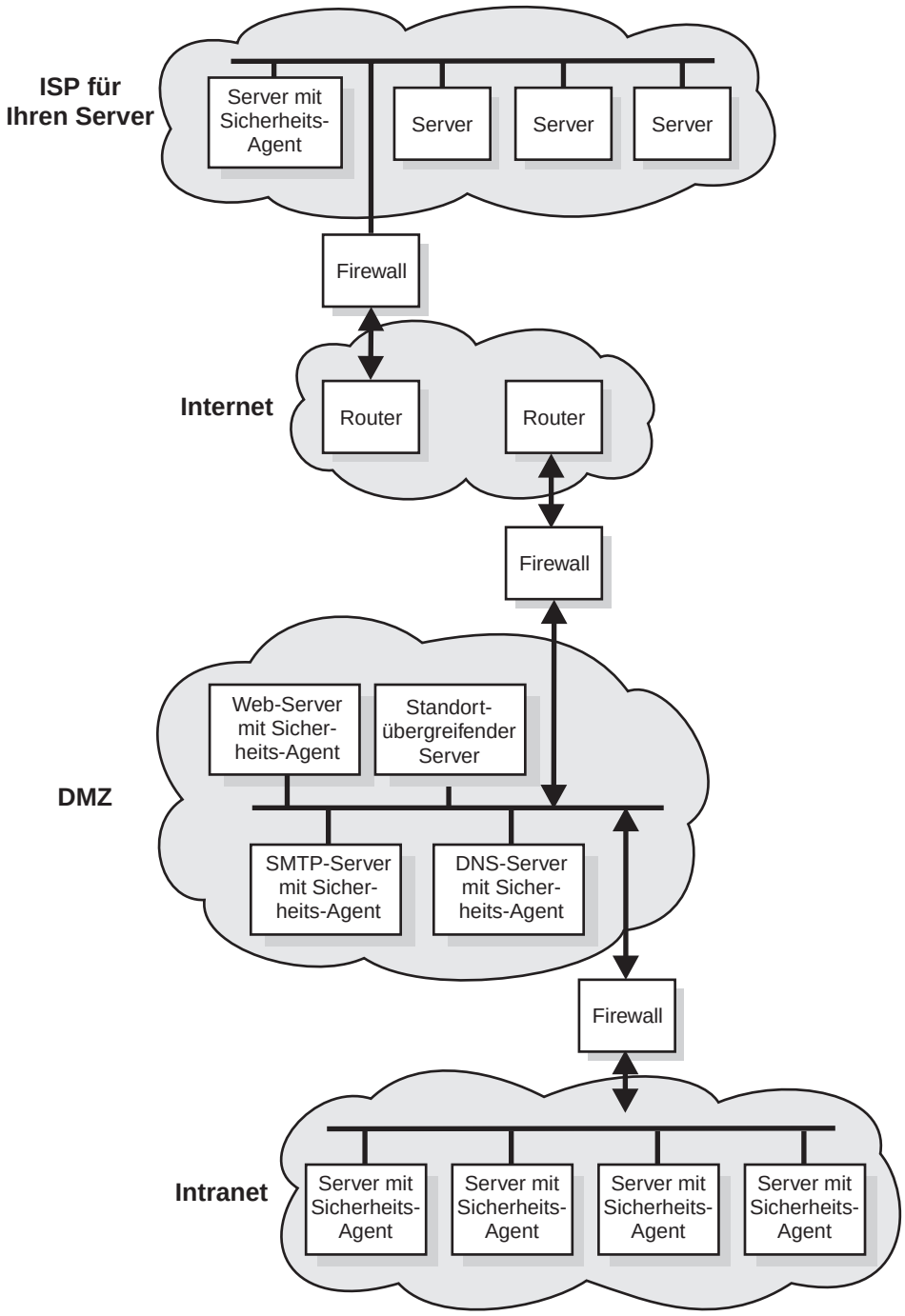


Abbildung 13. Installation des Cross-Site for Security-Verwaltungs-Servers in der DMZ mit Unterstützung eines an das Internet angeschlossenen Servers

Norton AntiVirus - Installationsvoraussetzungen

Informationen über die Installation von Norton AntiVirus stehen in der Datei contents.txt, die sich im Stammverzeichnis der Produkt-CD befindet.

Kapitel 14. Public Key Infrastructure - Voraussetzungen und Überlegungen zur Installation

Unternehmen benötigen heute zum Schutz von e-business-Anwendungen eine Infrastruktur mit allgemeinen Schlüsseln (Public Key Infrastructure). FirstSecure Trust Authority liefert zwei Funktionsebenen, mit denen eine Infrastruktur mit allgemeinen Schlüsseln implementiert wird:

- Verwaltung digitaler Zertifikate während ihrer gesamten Lebensdauer durch
  - — die Fähigkeit zum Anfordern, Erneuern und Widerrufen von Zertifikaten.
  - — eine Registrierungsstelle zum Bestätigen von Zertifikatanforderungen.
  - — eine Zertifizierungsstelle zum Erstellen von digitalen Zertifikaten und Widerrufungslisten.
- Erweiterte Registrierungsfähigkeiten, damit Unternehmen ihre gesicherten e-business-Definitionseinheiten online registrieren können. Die Registrierungsanwendung baut auf den folgenden Prinzipien auf:
  - — Die ausgegebenen und verwalteten Zertifikate müssen den Sicherheitsvoraussetzungen entsprechen, die bei sensiblen e-business-Anwendungen erforderlich sind, und die Registrierungsstelle muß denselben hohen Sicherheitsanforderungen entsprechen.
  - — Die Anwendung muß bei Bedarf eine Vielzahl von Registrierungsrichtlinien unterstützen (einschließlich der manuellen oder automatisierten Genehmigungen), eine flexible, standortunabhängige Authentifizierung bereitstellen und die Möglichkeit zum Isolieren von Registrierungsrichtlinien in separaten gesicherten Domänen bieten.

Das Authentifizierungsmodell ist bei der Gewährleistung der Zugriffssteuerung, Vertraulichkeit, Integrität und Nachprüfbarkeit der Quelle elektronischer Transaktionen hilfreich. Durch digitale Verschlüsselung, Zertifizierung und Unterschriften ermöglicht Trust Authority ein gesichertes e-business über das Internet, ein Intranet oder ein virtuelles privates Netz. Zur Verbesserung der Sicherheit des Unterschriftenschlüssels ist die Zertifizierungsstelle so konzipiert, daß sie mit Verschlüsselungshardware arbeiten kann.

Trust Authority-Server - Hardware- und Softwarevoraussetzungen

Die Server-Softwarevoraussetzungen für die Komponente Trust Authority sind in Tabelle 10 aufgeführt.

Tabelle 10 (Seite 1 von 2). Voraussetzungen für die Server-Software und wahlfreie Hardware für die Public Key Infrastructure-Komponente Trust Authority

Produkt	**Anmerkungen**
Eines der folgenden Betriebssysteme: • IBM AIX/6000 (AIX) Version 4.3.2 • Microsoft Windows NT Version 4.0 mit Service Pack 5	• Erforderlich. • Alle Trust Authority-Server-Programme müssen auf derselben Plattform installiert werden. AIX- und Windows NT-Maschinen können in derselben Systemkonfiguration nicht gemischt werden.
IBM SecureWay Directory Version 3.1.1	• Erforderlich. Integration mit Trust Authority-Code. • Bei der Installation von Trust Authority können Sie die Directory-Software auf der Maschine installieren, auf der auch Trust Authority installiert wird, oder Sie können die Directory-Software auf einer fernen Maschine installieren.
IBM WebSphere Application Server Version 2.02, Standard Edition. Beinhaltet IBM HTTP Server Version 1.3.3 und Sun Java Development Kit (JDK) 1.1.7.	• Erforderlich. Im Trust Authority-Datenträgerpaket enthalten. • Vor der Installation von Trust Authority müssen Sie die Web-Server-Software auf der Maschine installieren, auf der auch die Trust Authority- und Trust Authority-Server-Software installiert werden soll.
IBM DB2 Universal Database Enterprise Edition Version 5.2 mit Wartungs-Patch-Code 9.	• Erforderlich. Im Trust Authority-Datenträgerpaket enthalten. • Für jede Server-Komponente ist ein eindeutiges Datenbankexemplar vorhanden. Vor der Installation von Trust Authority müssen Sie DB2 auf allen Maschinen installieren, die als Trust Authority-Server benutzt werden sollen.

Tabelle 10 (Seite 2 von 2). Voraussetzungen für die Server-Software und wahlfreie Hardware für die Public Key Infrastructure-Komponente Trust Authority

Produkt	Anmerkungen
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, Modell 001 • IBM SecureWay 4758 CCA Support Program, Version 1.3.0.0 mit Wartungs-Patch-Code 1.3.0.1	• *Wahlfrei*. Nur für AIX-Systeme verfügbar. Sie müssen dieses Produkt über die normalen IBM Bestellkanäle bestellen. • Vor der Installation von Trust Authority müssen Sie die 4758-Hardware und das 4758-Unterstützungsprogramm auf dem Server installieren, auf dem auch die Trust Authority-Zertifizierungsstelle installiert werden soll. • Für die 4758-Verschlüsselungskarte ist ein PCI-Bus auf der RS/6000-Maschine erforderlich.

In Tabelle 11 und Tabelle 12 auf Seite 83 sind die Server-Hardwarevoraussetzungen für Trust Authority aufgeführt.

In Tabelle 11 und Tabelle 12 auf Seite 83 gilt folgendes:

- Eine kleine Produktionsumgebung gibt täglich Hunderte von Zertifikaten aus.
- Eine mittlere Produktionsumgebung gibt täglich mehrere Tausend Zertifikate aus.
- Eine große Produktionsumgebung gibt täglich etliche Tausend Zertifikate aus. Es kann sich zudem um ein System handeln, das Zertifizierungsstellenservices für andere Organisationen übernimmt.

Wollen Sie TrustAuthority unter Windows NT benutzen, empfiehlt IBM, Trust Authority auf einem IBM Netfinity-Server zu installieren. In der folgenden Tabelle sind Empfehlungen hinsichtlich der Systemgröße aufgeführt, die auf der Anzahl von Zertifikaten basieren, die von einer Trust Authority-Zertifizierungsstelle ausgegeben werden sollen.

Tabelle 11 (Seite 1 von 2). Beispielkonfiguration für eine Windows NT-Maschine

Maschinentyp	Prozessoren	Plattenspeicherplatz	Hauptspeicher
Kleine Produktionsumgebung			
Netfinity 3000	1 (450 MHz, Pentium II)	2 Laufwerke (9,1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 Laufwerke (9,1 GB)	512 MB

Tabelle 11 (Seite 2 von 2). Beispielkonfiguration für eine Windows NT-Maschine

Maschinentyp	**Prozessoren**	**Plattenspeicherplatz**	**Hauptspeicher**
Mittlere Produktionsumgebung			
Netfinity 3000	1 (500 MHz, Pentium III)	4 Laufwerke (18,2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 Laufwerke (9,1 GB)	1 GB
Große Produktionsumgebung			
Netfinity 5500	2 (450 MHz, Pentium III)	4 Laufwerke (9,1 GB, Hochgeschwindigkeitslaufwerk)	1 GB
Netfinity 5500	4 (500 MHz, Pentium III Xeon mit L2-Cache, 1024 KB)	4 Laufwerke (9,1 GB, Hochgeschwindigkeitslaufwerk)	1 GB
Netfinity 7000	2 (500 MHz, Pentium III mit L2-Cache, 512 KB)	4 Laufwerke (9,1 GB, Hochgeschwindigkeitslaufwerk)	1 GB
Netfinity 7000	4 (500 MHz, Pentium III Xeon mit L2-Cache, 1024 KB)	4 Laufwerke (18,2 GB)	2 GB

Wollen Sie TrustAuthority unter AIX benutzen, müssen Sie Trust Authority auf einer IBM RS/6000-Maschine installieren. In der folgenden Tabelle sind Empfehlungen hinsichtlich der Systemgröße aufgeführt, die auf der Anzahl von Zertifikaten basieren, die von einer Trust Authority-Zertifizierungsstelle ausgegeben werden sollen.

Tabelle 12. Beispielhardwarekonfiguration für eine AIX-Maschine

Maschinentyp	**Prozessoren**	**Plattenspeicherplatz**	**Hauptspeicher**
Kleine Produktionsumgebung			
F40	2 (233 MHz)	2 Laufwerke (9,1-GB-Ultra-2-Fast/Wide)	512 MB
Mittlere Produktionsumgebung			
F40	2 (233 MHz)	3 Laufwerke (9,1-GB-Ultra-2-Fast/Wide)	1 GB
Große Produktionsumgebung			
F50	4 (332 MHz)	5 Laufwerke (ein 9,1-GB-Ultra-2-Fast/Wide-Laufwerk plus vier 9,1-GB-SSA-Laufwerke)	2 GB
H50	4 (332 MHz)	5 Laufwerke (ein 9,1-GB-Ultra-2-Fast/Wide-Laufwerk plus vier 9,1-GB-SSA-Laufwerke)	2 GB
R50	6 (200 MHz)	2 Laufwerke (9,1-GB-Ultra-2-Fast/Wide)	1 GB
R50	8 (200 MHz)	5 Laufwerke (ein 9,1-GB-Ultra-2-Fast/Wide-Laufwerk plus ein 7133-SSA-Gehäuse mit vier 9,1-GB-SSA-Laufwerken)	2 GB

Trust Authority-Client - Hardware- und Softwarevoraussetzungen

IBM empfiehlt die folgende Workstation-Konfiguration für die Benutzung der Browser-Registrierungsformulare und zur Ausführung der Trust Authority-Client-Anwendung.

- Folgende Konfiguration der physischen Maschine:
  - Mindestens Intel-486-Prozessor mit 166 MHz und 32 MB Hauptspeicher (Intel-Pentium-Prozessor mit 200 MHz und mindestens 64 MB Hauptspeicher wird empfohlen)
  - Grafikkarte
  - Mindestens ein VGA-Video-Bildschirm
  - Maus oder mauskompatible Zeigereinheit
- Eines der folgenden Betriebssysteme:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT Version 4.0
- Einen der folgenden Web-Browser:
  - Netscape Navigator oder Netscape Communicator Version 3.0 oder höher
  - Microsoft Internet Explorer Version 4.0 oder höher mit aktiviertem Java

Interaktion von IBM KeyWorks Toolkit und IBM SecureWay Trust Authority

Installieren Sie IBM KeyWorks Toolkit nicht auf demselben Server wie IBM SecureWay Trust Authority.

Kapitel 15. Toolbox - Voraussetzungen und Überlegungen zur Installation

FirstSecure Toolbox ist eine Gruppe von APIs, die beim Entwickeln von gesicherten e-business-Anwendungen hilfreich sind und folgendes bieten:

- Berechtigungsservices
- Zertifizierungs- und Verwaltungsservices
- Verzeichnisservices
- Secure Sockets Layer-Protokollservices
- KeyWorks-Services für Verschlüsselungs- und Authentifizierungsverwaltung
  - — IBM Key Recovery Service Provider 1.1.3.0-APIs. Der IBM Key Recovery Service Provider ermöglicht die Wiederherstellung verschlüsselter Informationen.
  - — IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0 ist eine Anwendung, die nach einer berechtigten Anforderung verschlüsselte Informationen wiederherstellen kann, wenn Schlüssel unverfügbar, verlorengegangen oder beschädigt sind.

    Diese beiden Toolkits bieten Standardschnittstellen, über die Anwendungen kritische Sicherheitsservices aufrufen und Anbieter von Sicherheitsprodukten ihre Produkte in das Toolkit integrieren können. Die Standardschnittstellen basieren auf der CDSA-Architektur (CDSA = Common Data Security Architecture). Diese Toolkits sind unter Windows NT, Solaris und AIX verfügbar.

Toolbox - Hardware- und Softwarevoraussetzungen

Die Hardwarevoraussetzungen für die Toolbox werden in Tabelle 13 gezeigt.

Tabelle 13. Hardwarevoraussetzungen für die Toolbox

Plattform	Plattenspeicherplatz	Hauptspeicher
Version 4.0, Service Pack 5	2 - 4 GB	64 MB
AIX 4.3.2	9,1 GB	1 GB
Sun Solaris, Version 2.6 mit Fix Pak vom Mai 1999	4,2 GB	128 MB

Tabelle 14. Hardwarevoraussetzungen für Toolbox-Komponenten

Toolkit	**Maschinentyp**	**Plattenspeicher-platz**	**Hauptspeicher**
IBM KeyWorks Toolkit	Hardware für Produkte, die unter folgenden Betriebssystemen laufen: Windows NT Version 4.0, Service Pack 5 oder höher Windows 95 AIX 4.2 oder höher Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	Hardware für Produkte, die unter folgenden Betriebssystemen laufen: Windows NT Version 4.0, Service Pack 5 oder höher Windows 95 AIX 4.2 oder höher Sun Solaris	50 MB	32 MB

In der folgenden Tabelle sind die Softwarevoraussetzungen für die Toolbox-Komponenten aufgeführt.

Tabelle 15. Softwarevoraussetzungen für Toolbox-Komponenten

Toolbox-Komponente	**Microsoft Windows-Plattformen**		**AIX**	**Solaris**
	Client	**Server**	**Server**	**Server**
IBM KeyWorks Toolkit	Windows NT Version 4.0, Service Pack 5 oder höher Windows 95	Windows NT Version 4.0, Service Pack 5 oder höher Windows 95	AIX 4.2 oder höher[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT Version 4.0, Service Pack 5 oder höher[2] Windows 95	Windows NT Version 4.0, Service Pack 5 oder höher	AIX 4.2 oder höher	Sun Solaris

Anmerkungen:

1. Der AIX-Client wird ebenfalls unterstützt.
2. Zudem ist IBM KeyWorks Toolkit erforderlich.

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1 bietet Anwendungsentwicklern ein offenes, erweiterbares und standardisiertes Instrument zum Zugriff auf Verschlüsselungsfunktionen und andere Sicherheitsfunktionen zwischen unterschiedlichen Betriebsumgebungen.

IBM KeyWorks Toolkit bietet Standardschnittstellen (APIs), die Anwendungen zum Aufrufen wichtiger Verschlüsselungs-, Authentifizierungs- und Sicherheitsservices und Service Provider-Add-In-Module als Schnittstelle zu dem Toolkit benutzen können. Diese Standardschnittstellen basieren auf der CDSA-Architektur (Common Data Security Architecture), einem Standard der Open Group, der zunächst von der Intel Corporation entwickelt und dann von IBM im KeyWorks Toolkit erweitert wurde. Werden diese Standardschnittstellen benutzt,

- kann die Verschlüsselungs- und Authentifizierungsimplementierung ausgewählt werden, die am besten für das Unternehmen geeignet ist, ohne daß Änderungen an Anwendungen erforderlich sind, die die Sicherheitsservices benutzen.
- wird die Produktivität der Anwendungsprogrammierer und Middleware-Programmierer erhöht.

IBM KeyWorks Toolkit bietet eine Isolationsschicht zwischen Anwendungen und Middleware als Klasse und den Verschlüsselungsfunktionen und Service Providern. Das Toolkit enthält ein Gerüst und Service Provider-Plug-In-Module.

Für Anwendungen liefert das Gerüst die leistungsfähige CSSM-API (Common Secu-
rity Services Manager API) der CDSA-Architektur (Common Data Security Architecture) der Intel Corporation. IBM hat die CSSM-API erweitert und Funktionen zur Schlüsselwiederherstellung hinzugefügt. Wird IBM KeyWorks Toolkit benutzt, kann die Anwendung

- Informationen verschlüsseln und entschlüsseln
- digitale Unterschriften für verschiedene Zwecke überprüfen
- Zertifikate und Zertifikatwiderrufungslisten aus Verzeichnissen abrufen
- zwecks Schlüsselwiederherstellung und Verschlüsselungssicherung Felder zur Schlüsselwiederherstellung erstellen
- entscheiden, ob ein Zertifikat anhand von Kriterien, die von Systemdesignern und -programmierern auf Anweisung von Benutzern eingerichtet wurden, als sicher eingestuft wird

Normalerweise integriert ein Unternehmen oder ein OEM die Produkte IBM KeyWorks Toolkit und IBM Key Recovery Service Provider Toolkit so in Anwendungen und Middleware, daß die CSSM-APIs auf dem CSSM-Gerüst benutzt werden können. Das Ergebnis dieser Integration ist eine Gruppe von Laufzeitanwendungen und Middleware für Server und Clients, die innerhalb der Betriebsumgebung(en) verteilt werden. Die anderen FirstSecure-Elemente hängen in der Zwischenzeit bei allen Verschlüsselungsservices und Operationen, die die Sicherheitsrichtlinien betreffen, von IBM KeyWorks Toolkit ab.

Wird bei der Integration IBM KeyWorks Toolkit benutzt, müssen Systemberater und Systemprogrammierer verfügbar sein, die große Erfahrung mit dem Entwurf und der Programmierung von Verschlüsselungsfunktionen sowie mit Middleware und Gerüsten haben, oder es muß auf Vertragsfirmen oder OEMs zurückgegriffen werden, die eine solche Erfahrung aufweisen.

Für Service Provider liefert das Gerüst die Standard-SPI (Service Provider Interface) CDSA der Open Group. IBM hat die SPI durch Funktionen zur Schlüsselwiederherstellung erweitert.

IBM KeyWorks Toolkit (SDK) enthält Service-Provider-Plug-In-Module, die offene Standards und private Zertifikate für allgemeine Schlüssel unterstützen. Diese Module enthalten PKCS#11, die BSAFE-Verschlüsselungsfunktionen der RSA Data Security, X.509V3-Zertifikate, die Authentifizierungsrichtlinien von Entrust und Verisign sowie das LDAP-Protokoll (Lightweight Directory Access Protocol). Das Gerüst ermöglicht eine nahtlose Integration der Verschlüsselungs-, Authentifizierungs- und Sicherheitsfunktionen, die über die Module unabhängiger Service Provider zur Verfügung stehen.

IBM KeyWorks Toolkit kann wichtige Verwaltungsfunktionen liefern, einschließlich

- Schutzfunktionen, mit denen das Umgehen wichtiger Schritte in einem von KeyWorks unterstützten Prozeß verhindert wird
- Überprüfungsfunktionen, mit denen festgestellt wird, ob Service Provider-Plug-In-Module vor der Verwendung geändert wurden
- Benutzung der Service Provider-Plug-In-Module nur über das Gerüst
- Unterstützung für die landesspezifische und unternehmensspezifische Anwendung der Verschlüsselungs- und Sicherheitsrichtlinien

IBM KeyWorks Toolkit bietet die folgenden Vorteile:

- Möglichkeit zum Ändern oder Ersetzen von Service Provider-Modulen, ohne daß Anwendungen und Middleware neu geschrieben werden müssen
- Nahtlose Unterstützung für Hardwareverschlüsselung und digitale Unterschrift
- Unterstützung für LDAP-Verzeichnisse und den DSA-Unterschriftenstandard
- Es muß keine bestimmte Zertifizierungsstelle benutzt werden

Weitere Informationen über IBM KeyWorks Toolkit stehen im Buch *IBM KeyWorks Toolkit Developer's Guide.*

Interaktion von IBM KeyWorks Toolkit und IBM SecureWay Trust Authority

Installieren Sie IBM KeyWorks Toolkit nicht auf demselben Server wie IBM SecureWay Trust Authority.

IBM Key Recovery Service Provider Toolkit 1.1

IBM Key Recovery Service Provider 1.1.3.0 hat Toolkit-Format und ist ein Service Provider-Modul, das die Standardfunktionen von IBM KeyWorks Toolkit benutzt. IBM Key Recovery Service Provider ermöglicht die Wiederherstellung gespeicherter oder übertragener verschlüsselter Informationen, ohne daß persönliche Schlüssel gesammelt und verteilt werden müssen und daher einzelne Punkte zu einer Gefahr für die Verschlüsselung werden können.

Da IBM Key Recovery Service Provider die Standardfunktionen von IBM KeyWorks Toolkit verwendet, kann die Funktion zur Schlüsselwiederherstellung mit Verschlüsselungsprodukten unterschiedlicher Anbieter, Standardzertifikaten von verschiedenen Zertifizierungsstellen, den Authentifizierungsrichtlinien von Verisign und Entrust und allen Verzeichnissen benutzt werden, auf die mit LDAP (Lightweight Directory Access Protocol) zugegriffen werden kann. IBM Key Recovery Service Provider erstellt Informationen zur Schlüsselwiederherstellung anhand des Sitzungsschlüssels für die Kommunikation.

Weitere Informationen über IBM Key Recovery Service Provider enthält das Buch *Key Recovery Server Installation and Usage Guide*, das mit dem FirstSecure-Dokumentationspaket geliefert wird.

Kapitel 16. Mit FirstSecure gelieferte Dokumentationen

Alle zu FirstSecure gehörenden Komponenten werden mit eigenen Dokumentationen geliefert. Dieses Kapitel enthält Informationen über die mit den einzelnen FirstSecure-Komponenten gelieferten Dokumentationen.

Für SecureWay FirstSecure, SecureWay Policy Director und SecureWay Boundary Server ist jeweils ein Datenträgerpaket und ein Dokumentationspaket verfügbar. Datenträgerpakete enthalten Produkt-CDs, mit denen die zu dem Angebot gehörenden Komponenten installiert werden. Zudem befinden sich auf einigen dieser CDs Online-Dokumentationen. Dokumentationspakete enthalten gedruckte Bücher (Hardcopy-Bücher) zu den Produkten.

In „FirstSecure-Dokumentationspaket“ auf Seite 100 ist der Inhalt der Dokumentationspakete aufgeführt.

Policy Director

Die folgenden Dokumentationen werden mit den Policy Director-Komponenten geliefert.

IBM SecureWay Policy Director Installation und Konfiguration
: Diese Dokumentation enthält Informationen über die Installation und Konfiguration des IBM SecureWay Policy Director.

IBM SecureWay Policy Director Administration Guide
: Diese Dokumentation enthält Informationen über die Verwaltung des IBM SecureWay Policy Director. Dieses Buch ist in PDF-Format verfügbar.

IBM SecureWay Policy Director Programming Guide and Reference
: Diese Dokumentation enthält Informationen über das Schreiben von Programmen für den IBM SecureWay Policy Director. Dieses Buch ist in PDF-Format verfügbar.

Informationsdatei
: Diese Informationen stehen auf dem Web unter www.ibm.com/software/security/policy zur Verfügung.

SecureWay Boundary Server

In dem folgenden Buch werden die SecureWay Boundary Server-Komponenten, ihre Voraussetzungen und Interaktionen beschrieben.

IBM SecureWay Boundary Server für Windows NT und AIX: Installation und Konfiguration
Dieses Buch liegt in gedruckter Form vor und enthält Beschreibungen der SecureWay Boundary Server-Komponenten.

In den folgenden Abschnitten sind die mit den SecureWay Boundary Server-Komponenten gelieferten Dokumentationen beschrieben.

IBM SecureWay Firewall

Alle IBM Firewall-Dokumentationen sind als Softcopy verfügbar. Zu IBM Firewall gehören die folgenden Dokumentationen:

IBM SecureWay Firewall für AIX Konfiguration und Installation
Diese Dokumentation enthält Informationen über die Installation und Konfiguration von IBM SecureWay Firewall für AIX.

IBM SecureWay Firewall für Windows NT Konfiguration und Installation
Diese Dokumentation enthält Informationen über die Installation und Konfiguration von IBM SecureWay Firewall für Windows NT.

IBM SecureWay Firewall für AIX Benutzerhandbuch
Diese Dokumentation enthält Informationen über die Benutzung von IBM Firewall für AIX.

IBM SecureWay Firewall für Windows NT Benutzerhandbuch
Diese Dokumentation enthält Informationen über die Benutzung von IBM Firewall für Windows NT.

IBM SecureWay Firewall für Windows NT Referenzhandbuch
Diese Dokumentation enthält Referenzmaterial über die Benutzung von IBM Firewall für Windows NT.

IBM SecureWay Firewall für AIX Referenzhandbuch
Diese Dokumentation enthält Referenzmaterial über die Benutzung von IBM Firewall für AIX.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX
Diese Dokumentation enthält Anweisungen für die Fehlerbestimmung.

IBM SecureWay Firewall VPN Client User's Guide
Diese Dokumentation enthält Informationen über die Konfiguration und Benutzung eines virtuellen privaten Netzes.

MIMEsweeper

Zu MIMEsweeper gehören die folgenden Dokumentationen:

MIMEsweeper Administrator's Guide
: Dieses Buch enthält einen Abschnitt "Release Notes", gefolgt von Informationen für den Administrator, zu denen auch Informationen für die Planung und Installation gehören.

  Dieses Buch ist auf der Produkt-CD in HTML-Format verfügbar. Es kann online mit einem Web-Browser durch Aufrufen der Datei \DOC\MANUAL.HTM angezeigt werden.

MIMEsweeper Release Notes
: Diese Dokumentation enthält aktualisierte Informationen einschließlich der Informationen über die Installation und Anweisungen zum Anzeigen der Online-Dokumentation.

  Diese Dokumentation ist auf der Produkt-CD in HTML-Format verfügbar und kann online mit einem Web-Browser durch Aufrufen der Datei \DOC\RELNOTES.HTM angezeigt werden.

MIMEsweeper Configuration Editor Help
: Dieses Dokument enthält Informationen über das Bearbeiten der MIMEsweeper-Konfigurationsdateien.

  Dieses Dokument ist auf der Produkt-CD in HTML-Format verfügbar.

SurfinGate

Zu SurfinGate gehören die folgenden Softcopy-Dokumentationen:

SurfinGate Installation Guide
: Diese Dokumentation enthält Informationen über die Installation und Konfiguration der SurfinGate 4.05-Komponenten unter Windows NT. Es steht eine PDF-Version des Buchs *SurfinGate Installation Guide* zur Verfügung. Sie befindet sich auf der Produkt-CD in der folgenden Datei: \docs\install.pdf.

SurfinGate User Guide
: Diese Dokumentation enthält Informationen über die Planung und Benutzung von SurfinGate. Es steht eine PDF-Version des Buchs *SurfinGate User Guide* zur Verfügung. Sie befindet sich auf der Produkt-CD in der folgenden Datei: \docs\manual.pdf.

SurfinGate 4.05 for Windows NT Release Notes
: Diese Dokumentation enthält Informationen über SurfinGate 4.05 einschließlich der Systemvoraussetzungen und der Einschränkungen für das Produkt. Es steht eine PDF-Version der *SurfinGate 4.05 for Windows NT Release Notes* zur Verfügung. Sie befindet sich auf der Produkt-CD in der folgenden Datei: \docs\relnotes.pdf.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A
Diese Dokumentation ist ein Online-Dokument, in dem die Änderungen an SurfinGate erklärt sind. Dieses Dokument befindet sich auf der Produkt-CD in der folgenden Datei: \docs\rnappen.pdf.

Intrusion Immunity

In den folgenden Abschnitten sind die mit der Intrusion Immunity-Komponente gelieferten Dokumentationen beschrieben.

Tivoli Cross-Site for Security

Zu Tivoli Cross-Site for Security Version 1.1 gehören die folgenden Dokumentationen in PDF-Format:

Tivoli Cross-Site for Security Installation
In diesem Dokument werden die Installationsvoraussetzungen aufgeführt und die Installationsschritte beschrieben.

Tivoli Cross-Site for Security User's Guide
Dieses Dokument enthält eine Produktübersicht, Anweisungen zur Benutzung der Konsole und zur Ausführung von Aufgaben, Referenzinformationen wie Befehlszeilenschnittstellen, Informationen über die Konfigurationsdateien und ein Glossar. Auf dieses Dokument kann über die CD-ROM zugegriffen werden.

Norton AntiVirus

Norton AntiVirus enthält die folgenden Dokumentationen für von FirstSecure unterstützte Komponenten. Alle Dokumente mit Ausnahme der Datei contents.txt werden in PDF-Format auf der Norton AntiVirus-CD geliefert. Die Datei contents.txt ist eine ASCII-Datei auf der Produkt-CD.

Dokumentationen auf der Norton AntiVirus Solution Release 3.04-CD

In der auf der Norton AntiVirus Solution Release 3.04-CD befindlichen Datei \contents.txt sind alle auf der CD vorhandenen Dokumentationen aufgeführt.

Verwaltungslösungen

Norton AntiVirus Solution Implementation Guide
Siehe \docs\admin\navimp.pdf auf der Produkt-CD.

Norton AntiVirus Command-Line Scanner
Siehe \docs\navc\navcugd.pdf auf der Produkt-CD.

Emergency Rescue Disk creation
Siehe \navc\readme.txt auf der Produkt-CD.

Server-Lösungen

Norton AntiVirus for Windows NT Server Administrator's Guide
Siehe \docs\admin\navnts50.pdf auf der Produkt-CD.

Norton AntiVirus for NetWare User's Guide
Siehe \docs\NAVNLM\NVN4.pdf auf der Produkt-CD.

Norton AntiVirus for Lotus Notes Installation Guide
Siehe \docs\NAVNOTES\NAVNOTES.pdf auf der Produkt-CD.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide
Siehe \docs\NOTESOS2\NOTESOS2.pdf auf der Produkt-CD.

Norton AntiVirus for Microsoft Exchange Installation Guide
Siehe \docs\NAVXCHNG\NAVXCHNG.pdf auf der Produkt-CD.

Gateway-Lösungen

Norton AntiVirus for Internet Email Gateway User's Guide
Siehe \docs\navieg\navieg.pdf auf der Produkt-CD.

Norton AntiVirus for Firewalls Administrator's Guide
Siehe \docs\navfw\navfw.pdf auf der Produkt-CD.

Desktop-Lösungen

Norton AntiVirus User's Guide for Windows 3.1/DOS
Siehe \docs\navwks\nav4dusr.pdf auf der Produkt-CD.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
Siehe \docs\navwks\nav4dref.pdf auf der Produkt-CD.

Norton AntiVirus for Windows 95/98 User's Guide
Siehe \docs\navwks\nav98usr.pdf auf der Produkt-CD.

Norton AntiVirus for Windows 95/98 Reference Guide
Siehe \docs\navwks\nav98ref.pdf auf der Produkt-CD.

Norton AntiVirus for Windows NT User's Guide
Siehe \docs\navwks\nav5nusr.pdf auf der Produkt-CD.

Norton AntiVirus for Windows NT Reference Guide
Siehe \docs\navwks\nav5nref.pdf auf der Produkt-CD.

Norton AntiVirus v4.0 User's Guide for Windows NT
Siehe \docs\351\navntugd.pdf auf der Produkt-CD.

Norton AntiVirus v4.0 Reference Guide for Windows NT
Siehe \docs\351\navntref.pdf auf der Produkt-CD.

Norton AntiVirus User's Guide for OS/2
Siehe \docs\navos2\navos2ug.pdf auf der Produkt-CD.

Norton AntiVirus Distribution Guide for OS/2
Siehe \docs\navos2\navos2dg.pdf auf der Produkt-CD.

Norton AntiVirus for Macintosh User's Guide
Siehe \docs\navmac\navmac.pdf auf der Produkt-CD.

White Papers auf der Norton AntiVirus Solution Release 3.04-CD: Die CD enthält auch White Papers im Verzeichnis \sarc. Alle White Papers haben PDF-Format.

Videos auf der Norton AntiVirus Solution Release 3.04-CD: Auf der CD befinden sich auch Videos. Zum Anzeigen eines Videos muß Media Player oder ein anderes Programm installiert sein, das Dateien mit der Erweiterung AVI abspielen kann. Die Videos befinden sich in den folgenden Dateien:

SARC \sarc\sarc.avi

About Viruses
\sarc\aboutvir.avi

Norton AntiVirus: the Guided Tour
\navtour\guided\demo32.exe

How to Respond When Norton AntiVirus Alerts You
\navtour\alert\demo32.exe

A Tour of Norton System Center
\nsctour\setup.exe

Soll *A Tour of Norton System Center* direkt von der CD ausgeführt werden:

\nsctour\demo32.exe

Weitere Informationen über *A Tour of Norton System Center* befinden sich in der Datei \ncstour\readme.txt.

Trust Authority

Die IBM SecureWay Trust Authority-Produktdokumentationen sind in PDF- und HTML-Format auf der CD-ROM mit der Trust Authority-Dokumentation verfügbar. Einige Trust Authority-Dokumentationen wurden in andere Sprachen übersetzt. Anweisungen zum Zugriff auf eine Veröffentlichung in einer anderen Sprache als Englisch enthält die Informationsdatei *Readme* des Produkts. Die neueste Version der Informationsdatei *Readme* ist immer auf der Seite **Library** der IBM SecureWay Trust Authority-Web-Site verfügbar: http://www.ibm.com/software/security/trust/library.

Zu der Trust Authority-Bibliothek gehören die folgenden Dokumentationen:

IBM SecureWay Trust Authority Einführung
Dieses Buch enthält eine Übersicht über das Produkt. Es enthält die Produktvoraussetzungen, die Installationsprozeduren und Informationen über den Zugriff auf die für die einzelnen Komponenten verfügbare Online-Hilfefunktion. Dieses Buch befindet sich auf der Dokumentations-CD-ROM und wird auch als gedruckte Version mit dem Produkt geliefert.

IBM SecureWay Trust Authority Systemverwaltung
Dieses Buch enthält allgemeine Informationen über die Verwaltung des Trust Authority-Systems. Es beinhaltet Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zum Verwalten der Zertifizierungsstelle, zum Ausführen von Protokollierungen und zum Ausführen von Datenintegritätsprüfungen.

IBM SecureWay Trust Authority Konfiguration
Dieses Buch enthält Informationen über die Benutzung des Konfigurationsassistenten (Setup Wizard) zum Konfigurieren eines Trust Authority-Systems. Auf die HTML-Version dieses Buchs kann zugegriffen werden, wenn die Online-Hilfefunktion für den Konfigurationsassistenten (Setup Wizard) aufgerufen wird.

IBM SecureWay Trust Authority Registration Authority Desktop Guide
Dieses Buch enthält Informationen über die Benutzung des RA Desktop zur Verwaltung von Zertifikaten während der gesamten Lebensdauer von Zertifikaten. Auf die HTML-Version dieses Buchs kann zugegriffen werden, wenn die Online-Hilfefunktion für den Desktop aufgerufen wird.

IBM SecureWay Trust Authority Benutzerhandbuch
Dieses Buch enthält Informationen über den Erhalt von Zertifikaten. Es enthält Prozeduren zur Benutzung der Trust Authority-Registrierungsformulare zum Anfordern von Zertifikaten für Browser, Server und Einheiten. Zudem wird beschrieben, wie Benutzer sich vorab für ein PKIX-Zertifikat registrieren lassen können und wie mit dem Trust Authority-Client PKIX-Zertifikate gespeichert und verwaltet werden können. Auf die HTML-Version dieses Buchs kann zugegriffen werden, wenn die Online-Hilfefunktion für den Client aufgerufen wird.

Toolbox

In den folgenden Abschnitten sind die mit den Toolbox-Komponenten gelieferten Dokumentationen beschrieben.

Toolbox-APIs

Die gesamte Toolbox-Dokumentation ist auf der folgenden Web-Site verfügbar: `www.ibm.com/software/security/firstsecure/library`. Die folgenden Dokumentationen sind enthalten:

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference
Diese Dokumentation enthält eine Übersicht über APIs und iKeyman sowie eine Definition der einzelnen APIs einschließlich Syntax und Benutzung.

IBM SecureWay Directory Client SDK Programming Reference
Diese Dokumentation enthält verschiedene LDAP-Beispiel-Client-Programme und eine LDAP-Client-Bibliothek für den Anwendungszugriff auf die LDAP-Server. C und Java werden unterstützt.

IBM SecureWay Policy Director Programming Guide and Reference
Diese Dokumentation enthält eine Definition der einzelnen APIs einschließlich Syntax und Benutzung.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide
Diese Dokumentation enthält Installationsanweisungen und -voraussetzungen.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
Diese Dokumentation enthält Informationen für Programmierer, die Anwendungen mit der IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms (auch als PKIX bezeichnet) entwickeln. Sie enthält eine Übersicht über das Produkt, Anweisungen zum Schreiben von Programmen für separate PKIX-Komponenten und Beschreibungen der PKIX-APIs.

IBM KeyWorks Toolkit

Alle mit IBM KeyWorks Toolkit gelieferten Dokumentationen sind Online-Dokumentationen und in PDF-Format auf der Produkt-CD verfügbar.

Die folgenden Dokumentationen sind verfügbar:

IBM KeyWorks Toolkit Developer's Guide
Dieses Buch enthält eine Übersicht über das Toolkit. Es enthält zudem Erklärungen zur Integration des Toolkits in Anwendungen und eine Beispielanwendung.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
Diese Spezifikation enthält die Definition der Schnittstelle, die Anwendungsentwickler für den Zugriff auf Sicherheitsservices benutzen, die über das Gerüst und Service Provider-Module zur Verfügung stehen.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
In diesem Buch werden die Einrichtungen beschrieben, die bei allen Toolkit-Service Provider-Modulen gleich sind. Dieses Dokument muß zusammen mit den einzelnen Service Provider Interface Specifications benutzt werden, damit ein Service Provider-Modul aufgebaut werden kann.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
Diese Spezifikation enthält die Definition der Schnittstelle, der Service Provider-Module für die Verschlüsselung entsprechen müssen, damit über das Toolkit auf die Service Provider-Module zugegriffen werden kann.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
Diese Spezifikation enthält die Definition der Schnittstelle, der Service Provider-Module für die Schlüsselwiederherstellung entsprechen müssen, damit über das Toolkit auf die Service Provider-Module zugegriffen werden kann.

IBM KeyWorks Toolkit Trust Policy Interface Specification
Diese Spezifikation enthält die Definition der Schnittstelle, der Stellen für die Realisierung von Sicherheitsrichtlinien (z. B. Zertifizierungsstellen, Ausgeber von Zertifikaten und Anwendungsentwickler, die für die Realisierung von Sicherheitsrichtlinien zuständig sind) entsprechen müssen, damit das Toolkit mit modell- oder anwendungsspezifischen Richtlinien erweitert werden kann.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification
Diese Spezifikation enthält die Definition der Schnittstelle, der Entwickler für Zertifizierungsbibliotheken entsprechen müssen, damit formatspezifische Services zur Bearbeitung von Zertifikaten für die verschiedenen Toolkit-Anwendungen und Module für Authentifizierungsrichtlinien verfügbar sind.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification
Diese Spezifikation enthält die Definition der Schnittstelle, der Entwickler für Bibliotheken entsprechen müssen, damit ein formatspezifischer oder formatunabhängiger permanenter Speicher für Zertifikate verfügbar ist.

IBM Key Recovery Service Provider

Die folgende Dokumentation wird mit IBM Key Recovery Service Provider in PDF-Format auf der Produkt-CD geliefert:

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide
Dieses Buch enthält Informationen über Konzepte zur Schlüsselwiederherstellung, Anleitungen zum Aufbau einer Lösung für die Schlüsselwiederherstellung in einem Unternehmen und Prozeduren für die Installation, die Konfiguration und den Betrieb des IBM Key Recovery Server.

Redbooks über die Sicherheit

Die folgenden Reedbooks der IBM International Technical Support Organization (ITSO) enthalten Informationen zum Produkten und Prozessen für die Sicherheit. Sie sind unter www.us.ibm.com/redbooks verfügbar.

- *Understanding the IBM SecureWay FirstSecure Framework*
- *High Availability IBM eNetwork Firewall*

Dokumentationspakete

Die folgenden Dokumentationspakete sind für IBM SecureWay FirstSecure verfügbar.

FirstSecure-Dokumentationspaket

Das FirstSecure-Dokumentationspaket enthält die folgenden Bücher:

- FirstSecure-Lizenzinformationen
- *IBM SecureWay FirstSecure Planung und Integration*
- *IBM SecureWay Policy Director Installation und Konfiguration*
- *IBM SecureWay Boundary Server für Windows NT und AIX: Installation und Konfiguration*
- *IBM SecureWay Trust Authority Einführung*
- *Tivoli Cross-Site for Security Installation*

Policy Director-Dokumentationspaket

Das Policy Director-Dokumentationspaket enthält die folgenden Bücher:

- Policy Director-Lizenzinformationen
- *IBM SecureWay Policy Director Installation und Konfiguration*

SecureWay Boundary Server-Dokumentationspaket

Das SecureWay Boundary Server-Dokumentationspaket enthält die folgenden Bücher:

- SecureWay Boundary Server-Lizenzinformationen
- *IBM SecureWay Boundary Server für Windows NT und AIX: Installation und Konfiguration*

Teil 4. Anhänge

Anhang A. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an

IBM Europe
Director of Licensing
F-92066 Paris La Defense Cedex, France

zu richten.

Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekanntgegeben. Änderung des Textes bleibt vorbehalten.

Verweise in diesen Informationen auf Web-Sites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Web-Sites dar. Das über diese Web-Sites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Web-Sites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen

unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse (Anfragen an diese Adresse müssen auf englisch formuliert werden):

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der IBM Kundenvereinbarung (Internationale Nutzungsbedingungen der IBM für Programmpakete) oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Informationen dienen nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation:

AIX
AIX/6000
DB2
DB2 Universal Database
eNetwork
Global Sign-On
GSO
IBM
Netfinity
OS/2
RS/6000
SecureWay
Websphere

Intel und Pentium sind in gewissen Ländern Marken der Intel Corporation.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc..

Lotus, Lotus Notes, Domino und cc:Mail sind in gewissen Ländern Marken der Lotus Development Corporation.

Microsoft, Windows, Windows NT und das Logo von Windows sind in gewissen Ländern Marken der Microsoft Corporation.

Tivoli ist in gewissen Ländern eine Marke der Tivoli Systems Inc..

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

Glossar

In diesem Glossar werden neue oder wichtige Begriffe und Abkürzungen erklärt, die in diesem Buch vorkommen.

A

ACL. Access Control List (Zugriffssteuerungsliste).

ActiveX. In der Microsoft-Programmierung eine Gruppe von objektorientierten Technologien und Begriffen.

Agent. In Tivoli Cross-Site for Security ein intelligentes Überwachungsprogramm für IP-Pakete, das Pakete aufgreift, auf Abnormitäten auf unterschiedlichen Vermittlungsschichten überprüft und den Status der eingerichteten Verbindungen sowie Statistiken verfolgt.

Allgemeiner Schlüssel. Der Schlüssel eines Schlüsselpaars aus allgemeinem und persönlichem Schlüssel, der anderen zur Verfügung gestellt wird. Er ermöglicht es, eine Transaktion an den Eigner des Schlüssels zu übertragen oder eine digitale Unterschrift zu überprüfen. Mit einem allgemeinen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden persönlichen Schlüssel entschlüsselt werden. Siehe auch *Schlüsselpaar aus allgemeinem und persönlichen Schlüssel*.

Anwendungsprogrammierschnittstelle. Eine Funktionsschnittstelle, durch die ein in einer höheren Programmiersprache geschriebenes Anwendungsprogramm bestimmte Funktionen benutzen kann.

Apache-Server. Eine Gruppe von frei verfügbarer Web-Server-Software.

API. Application Programming Interface (Anwendungsprogrammierschnittstelle).

Assistent. Ein Dialog innerhalb einer Anwendung, der Benutzer anhand von Schrittfolgen durch eine bestimmte Aufgabe führt.

Authentifizierung. Der Prozeß zur zuverlässigen Ermittlung der Identität einer an der Kommunikation beteiligten Partei.

B

Berechtigung. Der Prozeß zur Festlegung der Arten von Aktivitäten, die ein Benutzer ausführen darf. Die Berechtigung erfolgt nach der Authentifizierung.

Bloodhound. In Norton AntiVirus-Produkten die Komponente zum Aufspüren von Viren.

C

Circiut-Level-Gateway. In einer Firewall ein Proxy-Server, der eine Client-Anforderung durch die Firewall an den vorgesehenen Server umleitet.

Client. (1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das einen Service eines anderen Computers oder Programms anfordert.

D

Dämon. In AIX ein Programm, das resident bleibt und darauf wartet, eine Serviceanforderung zu bedienen.

DCE. Distributed Computing Environment (Umgebung für verteilte Datenverarbeitung).

Digitales Zertifikat. Eine elektronische Berechtigung, die von einer Zertifizierungsstelle an eine Person oder Definitionseinheit ausgegeben wird. Ein Zertifikat enthält Informationen über die Definitionseinheit, die zertifiziert wird.

E

e-business. Das Durchführen von Geschäftstransaktionen über Netze und mit Computern, beispielsweise das Einkaufen und Verkaufen von Waren und Dienstleistungen und das Überweisen von Geldsummen durch digitale Kommunikation.

e-commerce. Das Durchführen von Geschäftstransaktionen, beispielsweise das Einkaufen und Verkaufen von Waren und Dienstleistungen im Internet. e-commerce ist das primäre Element des e-business.

Ereignis. In Tivoli Cross-Site for Security eine verdächtige Aktivität, die möglicherweise eine Attacke auf das System darstellt.

Extranet. Das Derivat des Internet, das eine ähnliche Technologie benutzt. Firmen nutzen zunehmend Web-Veröffentlichungen, e-commerce, das Senden von Nachrichten und Groupware für mehrere Benutzergemeinschaften von Kunden, Geschäftspartnern und Mitarbeitern.

F

Fernprozeduraufruf. (1) Eine Einrichtung, mit der ein Client die Ausführung eines Prozeduraufrufs von einem Server anfordert. Diese Einrichtung beinhaltet eine Bibliothek mit Prozeduren und eine externe Datendarstellung. (2) Eine Client-Anforderung für einen Service Provider auf einem anderen Knoten.

File Transfer Protocol (FTP).
Ein Client/Server-Internet-Protokoll, mit dem Dateien zwischen Computern übertragen werden können.

Filtern des Inhalts (Content Filtering). Das Auseinandernehmen des Inhalts einer Übertragung, damit der Inhalt gelesen werden kann, um festzustellen, ob eine Übertragung bestimmten Standards hinsichtlich des Inhalts entspricht.

Firewall. Ein System oder eine Kombination von Systemen zum Einrichten sicherer Grenzen zwischen Netzen.

G

Gateway. Ein System, das es inkompatiblen Netzen oder Anwendungen ermöglicht, miteinander zu kommunizieren.

H

Hacker. Eine Person, die ohne entsprechende Berechtigung versucht, auf eine Maschine oder ein System zuzugreifen. Hacker neigen dazu, Ressourcen unerlaubt zu nutzen.

I

IDE. Integrated Development Environment (integrierte Entwicklungsumgebung).

Implementierungsservices. Die Installationsunterstützung durch IBM vor Ort.

Integrierte Entwicklungsumgebung. Ein Programm zur Anwendungsentwicklung, mit dem Anwendungen codiert und mit Unterbrechungspunkten ausgeführt werden können und Diagnosehilfen für Programmfehler zur Verfügung stehen.

Internet. Eine weltweite Sammlung von Netzen, die die elektronische Kommunikation zwischen Computern ermöglicht. Die Kommunikation erfolgt über Softwareservices wie E-Mail oder Web-Browser. Bestimmte Universitäten sind beispielsweise an ein Netz angeschlossen, das wiederum mit anderen ähnlichen Netzen verbunden ist. Diese Netze bilden zusammen das Internet.

Intranet. Ein Netz innerhalb eines Unternehmens, das sich normalerweise hinter Firewalls befindet. Es ist ein Derivat des Internet, das eine ähnliche Technologie benutzt. Technisch ist ein Intranet eine reine Erweiterung des Internet. HTML (eine Sprache für die grafische Darstellung von Informationen) und HTTP (ein Protokoll, das Hypertext-Dateien im Internet transportiert) sind einige der Gemeinsamkeiten.

IntraVerse-Server. In IntraVerse ein System auf den Netz, das die IntraVerse-Server-Software enthält und mit allen Host-Systemen mit NetSEAT-Client-Software kommunizieren kann. Der IntraVerse-Server bezieht sich auf ein System

oder eine Kombination von Systemen, die die zu dem Produkt gehörenden Programme ausführen.

IPSec. Ein von der IETF (Internet Engineering Task Force) entwickelter Standard für die Sicherheit des Internet Protocol. IPSec ist ein Protokoll der Vermittlungsschicht für Sicherheitsservices zur Verschlüsselung, mit denen Kombinationen aus Authentifizierung, Integritätssicherung, Zugriffssteuerung und Vertraulichkeitssicherung flexibel unterstützt werden. Aufgrund seiner leistungsfähigen Authentifizierungsfunktionen wurde dieses Protokoll von vielen Anbietern von Produkten für virtuelle private Netze als Protokoll für gesicherte Punkt-zu-Punkt-Verbindungen über das Internet übernommen.

ISV. Independent Software Vendor (unabhängiger Softwarelieferant).

J

Java. Eine Gruppe von netzgestützten, plattformunabhängigen Computertechnologien, die von der Sun Microsystems, Incorporated, entwickelt wurden. Die Java-Umgebung besteht aus dem Java-Betriebssystem, den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Programmiersprache Java und mehreren Klassenbibliotheken.

JavaScript. Eine prozedurbasierte Sprache, die Java ähnlich ist und von Netscape für den Netscape-Browser entwickelt wurde.

K

Kanal. Ein Pfad, über den Signale gesendet werden können.

Kerberos. Eine gesicherte Methode zur Authentifizierung eines Services, der einen Computer anfordert. Kerberos wurde in dem Athena Project am Massachusetts Institute of Technology (MIT) entwickelt. In der griechischen Mythologie ist Kerberos ein Hund mit drei Köpfen, der das Tor zum Hades bewacht. Mit Kerberos kann ein Benutzer eine verschlüsselte Zugriffsberechtigung von einem Authentifizierungsprozeß anfordern, mit der dann ein bestimmter Service von einem Server angefordert werden kann. Das Kennwort des Benutzers muß nicht über das Netz übergeben werden.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol. Im IBM SecureWay Directory bietet LDAP eine Möglichkeit zum Verwalten von Verzeichnisinformationen an einem zentralen Standort (Speichern, Aktualisieren, Abrufen und Datenaustausch).

M

Makrobombe. Eine gesicherte Befehlsfolge, die an einen anderen Benutzer gesendet wird, um bei diesem Benutzer unerwünschte Ergebnisse hervorzurufen.

Minianwendung. Ein Computerprogramm, das in Java geschrieben ist und innerhalb eines Java-kompatiblen Browsers wie dem Netscape Navigator läuft. Sie wird auch als Java-Applet bezeichnet.

Mobiler Code. Datenverarbeitung auf einem tragbaren Computer durch einen Benutzer, der sich oft an verschiedenen Standorten befindet und unterschiedliche Arten von Netzverbindungen benutzt (beispielsweise Wählleitungen, LANs oder drahtlose Verbindungen).

MPEG. Der in der Entwicklung befindliche Standard der Moving Pictures Experts Group zum Komprimieren und Speichern von Bewegtbildvideo und -animation in digitaler Form.

N

Namensbereich. Hinsichtlich des SecureWay Directory die externe Struktur von Namen, auf die von Benutzern zugegriffen werden kann.

Netzadressenfilterung. Das Überprüfen der Adresse ankommender oder abgehender E-Mail, um festzustellen, ob der Empfänger oder Absender akzeptiert werden kann.

O

Object Request Broker. In der objektorientierten Programmierung Software, die als Vermittler dient, indem Objekte transparent Anforderungen und Antworten austauschen können.

OEM. Original Equipment Manufacturer.

P

Plug-In. Ein Programm, das als Teil des Web-Browsers benutzt werden kann.

Principal. In einer Umgebung für verteilte Datenverarbeitung (Distributed Computing Environment, DCE) eine Definitionseinheit, die über die DCE-Sicherheitsfunktionen sicher mit einer anderen Definitionseinheit kommunizieren kann. Principals können Benutzer, Server oder Computer sein.

Proxy-Server. Ein Vermittler zwischen dem Computer, der Zugriff anfordert (A), und dem Computer, auf den zugegriffen wird (B). Fordert ein Endbenutzer eine Ressource von Computer A an, wird diese Anforderung an einen Proxy-Server übergeben. Der Proxy-Server übernimmt die Anforderung, erhält eine Antwort von Computer B und leitet die Antwort dann an den Endbenutzer weiter. Proxy-Server sind beim Zugriff auf World Wide Web-Ressourcen innerhalb einer Firewall nützlich.

Prüfprotokoll. Daten in Form eines logischen Pfades, der eine Folge von Ereignissen verbindet. Ein Prüfprotokoll kann zum Verfolgen von Transaktionen oder der Statistik einer bestimmten Aktivität benutzt werden. Beispielsweise können die Aktivitäten eines Kundenkontos verfolgt werden.

R

RPC. Remote Procedure Call (Fernprozeduraufruf).

S

Schlüsselpaar aus allgemeinem und persönlichen Schlüssel. Ein Schlüsselpaar aus allgemeinem und persönlichen Schlüssel ist Teil des Konzepts der Verschlüsselung über Schlüsselpaare (1976 von Diffie und Hellman eingeführt, um das Problem der Schlüsselverwaltung zu lösen). In ihrem Konzept erhält jede Person ein Schlüsselpaar aus allgemeinem Schlüssel und persönlichem Schlüssel. Der allgemeine Schlüssel der einzelnen Personen wird veröffentlicht, während der persönliche Schlüssel geheim bleibt. Absender und Empfänger müssen geheime Informationen nicht gemeinsam benutzen. Für die gesamte Kommunikation sind nur allgemeine Schlüssel erforderlich, und die persönlichen Schlüssel werden nie übertragen oder gemeinsam benutzt. Bestimmte DFV-Kanäle müssen nicht mehr gesichert werden, um sie gegen unbefugte Zugriffe und Manipulation zu schützen. Die allgemeinen Schlüssel müssen ihren Benutzern lediglich in einer gesicherten (authentifizierbaren) Weise zugeordnet werden, beispielsweise in einem Authentifizierungsverzeichnis (Trusted Directory). Jeder kann anhand der allgemeinen Informationen eine vertrauliche Nachricht senden. Die Nachricht kann jedoch nur mit einem persönlichen Schlüssel entschlüsselt werden, der im Besitz des vorgesehenen Empfängers ist. Zudem kann die Verschlüsselung über Schlüsselpaare nicht nur zur Sicherung der Vertraulichkeit der Daten, sondern auch für die Authentifizierung (digitale Unterschriften) benutzt werden.

Secure Sockets Layer (SSL). (1) Ein IETF-DFV-Standardprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer so transparent wie möglich sind. Dieses Protokoll bietet gesicherte Kanäle für digitale Übertragung. (2) Ein SSL-fähiger Server akzeptiert normalerweise SSL-Verbindungsanforderungen auf einem anderen Anschluß als die Standard-HTTP-Anforderungen. SSL erstellt eine Sitzung, bei der der Handshake nur ein einziges Mal erfolgen muß. Ist der Handshake abgeschlossen, wird die Übertragung verschlüsselt. Bis zum Ende der SSL-Sitzung wird die Nachrichtenintegrität überprüft.

SecurID-Token.
Die ACE/Server-Authentifizierungsmethode der Security Dynamics beinhaltet eine Benutzer-ID und ein SecurID-Token. Bei einer Fernanmeldung erhält der Benutzer das Kennwort von dem SecurID-Token. Das Kennwort ändert sich alle 60 Sekunden und kann nur ein einziges Mal benutzt werden. Selbst wenn das Kennwort über das offene Netz abgefangen wird, kann es nicht zusätzlich verwendet werden.

Server. (1) In einem Netz eine Workstation, die anderen Workstations Einrichtungen zur Verfügung stellt, beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort bearbeitet (Client/Server).

SOCKS-Protokoll. Ein Protokoll, mit dem eine Anwendung in einem gesicherten Netz über eine Firewall über einen Socks-Server kommunizieren kann.

Socks-Server. Ein Circiut-Level-Gateway, der über eine Firewall eine gesicherte einseitige Verbindung zu Server-Anwendungen in einem ungesicherten Netz einrichten kann.

Spam. Unerwünschte E-Mail, die oft an eine Vielzahl von Empfängern gesendet wird.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

Telnet. In der Internet-Protokollgruppe ein Protokoll für den Service ferner Terminal-Verbindungen. Durch dieses Protokoll können Benutzer eines Hosts sich an einem fernen Host anmelden und als direkt angeschlossene Terminal-Benutzer dieses Hosts arbeiten.

Transmission Control Protocol/Internet Protocol. Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze und Weitverkehrsnetze unterstützen.

U

Überwachungssignal. Die Übertragung von einem Programm zu einem Verwaltungsprogramm zwecks Bestätigung der Aktivität. Das Programm teilt dem Verwaltungsprogramm mit, daß es noch aktiv ist und seine Aufgaben ausführt.

Umgebung für verteilte Datenverarbeitung (DCE). Services und Tools, die das Erstellen, Benutzen und Verwalten von verteilten Anwendungen in einer heterogenen Datenverarbeitungsumgebung unterstützen.

Unbestreitbarkeit der Unterschrift. Die Benutzung eines digitalen persönlichen Schlüssels, um zu verhindern, daß der Unterzeichner eines Dokuments bestreiten kann, das Dokument unterzeichnet zu haben, obwohl er es unterzeichnet hat.

Universal Resource Locator (URL). Die Namenskonvention, die für die Kommunikation über das World Wide Web benutzt wird und bei der der Pfad eines Web-Objekts mit dem Servicenamen, dem Namen des Unternehmens, dem Pfad und dem Dateinamen beginnt, beispielsweise http://www.ibm.com/software/security/firstsecure.

URL. Universal Resource Locator.

V

Vault. Ein Vault benutzt die Verschlüsselung zum Schutz von Informationen gegen unberechtigten Zugriff durch unbefugte Personen wie Systemadministratoren und Eigner anderer Vaults. Vaults benutzen zudem digitale Unterschriften als Schutz gegen Fälschungen und digitale Zertifizierung als Schutz gegen die Kommunikation mit unbekannten Parteien sowie die Verschlüsselung, digitale Unterschriften und Zertifizierung zur gesicherten Übertragung von Informationen an andere Vaults.

Verschlüsselung. Informationen so chiffrieren, daß die Originalinformationen nur entschlüsselt werden können, wenn der entsprechende Entschlüsselungscode verfügbar ist.

Virtuelles privates Netz. Ein privates Datennetz, das zum Einrichten von Fernverbindungen das

Internet und keine Telefonleitungen verwendet. Da der Benutzerzugriff auf Ressourcen im Unternehmensnetz über einen Internet Service Provider (ISP) und nicht über eine Telefongesellschaft erfolgt, können die Kosten für den Fernzugriff erheblich reduziert werden. Mit einem virtuellen privaten Netz (VPN) wird zudem die Sicherheit des Datenaustauschs erhöht. In der herkömmlichen Firewall-Technologie kann zwar der Inhalt einer Nachricht verschlüsselt werden, nicht aber die Quellen- und Zieladresse.

In der VPN-Technologie können Benutzer eine Tunnelverbindung einrichten, in der das gesamte Informationspaket (Inhalt und Kopfzeilenbereich) verschlüsselt und eingekapselt wird.

Virus. Ein Programm, das in der Lage ist, sich über ein Computernetz selbst zu kopieren und Schäden anzurichten.

VPN. Virtuelles privates Netz.

W

Web-Anwendung. Eine Anwendung für den Zugriff über das World Wide Web.

Web-Browser. Client-Software, die auf einem Desktop-PC läuft und mit der World Wide Web-Seiten und lokale Seiten angezeigt werden können. Sie ermöglicht den weltweiten Zugriff auf große Sammlungen von Hypermedia-Material im Web und Internet. Netscape Navigator und Microsoft Internet Explorer sind beispielsweise Web-Browser. Siehe auch *Server*.

Web-Objekt. Daten, die über einen Web-Browser verfügbar sind. Ein Web-Objekt kann eine Web-Seite, ein Teil einer Web-Seite, eine Datei, ein Abbild (Image), ein Verzeichnis, ein CGI-Programm oder eine Java-Minianwendung sein.

Web-Server. Ein Server-Programm, das Anforderungen für Informationsressourcen durch Browser-Programme beantwortet.

X

X.509. Ein weitverbreiteter Zertifikatstandard, der die gesicherte Verwaltung und Verteilung von PKI-Zertifikaten mit digitalen Unterschriften in gesicherten Internet-Netzen unterstützt. Das X.509-Zertifikat definiert Datenstrukturen mit Prozeduren, die sich auf die Verteilung von allgemeinen Schlüsseln beziehen, die von authentifizierten Dritten unterschrieben wurden.

Z

Zelle. In einer Umgebung für verteilte Datenverarbeitung (Distributed Computing Environment, DCE) eine Gruppe von Benutzern, Systemen und Ressourcen, die einem gemeinsamen Zweck dienen und gemeinsame Sicherheits-, Verwaltungs- und Benennungsgrenzen aufweisen. Die Zugriffsberechtigungen auf Elemente dieser Zelle sind für Benutzer, Maschinen und Ressourcen einer solchen Zelle untereinander normalerweise höher als für Benutzer, Maschinen und Ressourcen, die nicht Mitglied der Zelle sind.

Zellenverzeichnisservice. Eine Komponente einer Umgebung für verteilte Datenverarbeitung (Distributed Computing Environment, DCE), die eine Datenbank mit Informationen über Ressourcen innerhalb einer DCE-Zelle verwaltet.

Zertifizierungsstelle. Die Definitionseinheiten, Softwareanwendungen oder Personen, die für die Einhaltung der Sicherheitsrichtlinien eines Unternehmens und für die Zuordnung gesicherter elektronischer Identitäten in Form von Zertifikaten zuständig sind. Die Zertifizierungsstelle bearbeitet Anforderungen zum Ausgeben, Erneuern und Widerrufen von Zertifikaten.

Zugriffssteuerung. Hinsichtlich der Computersicherheit der Prozeß, mit dem sichergestellt wird, daß die Ressourcen eines Datenverarbeitungssystems nur von berechtigten Benutzern und auf der Basis der Ihnen erteilten Berechtigungen benutzt werden können.

Zugriffssteuerungsliste. Ein Mechanismus zur Begrenzung der Benutzung einer bestimmten Ressource für berechtigte Benutzer.

Index

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Antwort

IBM SecureWay First Secure
Planung und Integration
Version 2

IBM Teilenummer CT7EHDE

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Senden Sie Ihre Anregungen bitte an die angegebene Adresse.

IBM Deutschland
Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Kommentare:

Zu Ihrer weiteren Information:

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre *IBM Geschäftsstelle*, Ihren *IBM Geschäftspartner* oder Ihren *Händler*. Unsere Telefonauskunft **„Hallo IBM“** (Telefonnr.: 0180 3 / 31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Teilenummer: CT7EHDE

Printed in Denmark

CT7EHDE