IBM SecureWay Boundary Server
für Windows NT und AIX

Installation und Konfiguration

Version 2.0

IBM SecureWay Boundary Server
für Windows NT und AIX

Installation und Konfiguration

Version 2.0

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter Anhang B, „Bemerkungen“ auf Seite 47, gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM SecureWay Boundary Server for Windows NT and AIX Up and Running Version 2.0,
IBM Teilenummer CT6RZNA,

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.

Änderungen des Textes bleiben vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
Oktober 1999

Inhaltsverzeichnis

Zu diesem Handbuch

In diesem Buch wird die Installation, Konfiguration, Benutzung und Fehlerbehebung für den IBM SecureWay Boundary Server für Windows NT und AIX erklärt.

Zur Installation und Konfiguration des SecureWay Boundary Server sind gute Kenntnisse über Firewalls, virtuelle private Netze, Content Security und Netzverwaltung erforderlich. Da Sie eine Firewall installieren und konfigurieren, die den Zugriff auf das und aus dem Netz steuert, müssen Sie wissen, wie der Netzbetrieb funktioniert. Insbesondere müssen Sie grundlegende Kenntnisse über IP-Adressen, vollständig qualifizierte Namen und Teilnetzmasken haben.

Zielgruppe

Dieses Buch richtet sich an Administratoren für die Netz- und Systemsicherheit, die den IBM SecureWay Boundary Server installieren, verwalten und benutzen.

Jahr-2000-Fähigkeit

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 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.

Service und Unterstützung

Nehmen Sie Kontakt mit IBM auf, wenn Sie für ein Produkt des IBM SecureWay FirstSecure-Angebots Service und Unterstützung benötigen. In einigen dieser Produkte wird auf Unterstützung durch andere Anbieter als IBM verwiesen. Werden diese Produkte als Bestandteil des FirstSecure-Angebots geliefert, nehmen Sie Kontakt mit IBM auf, wenn Sie Service und Unterstützung benötigen.

Aufbau des Handbuchs

Dieses Buch besteht aus den folgenden Kapiteln:

- Kapitel 1, „Übersicht über den SecureWay Boundary Server“ auf Seite 1, enthält eine Übersicht über den SecureWay Boundary Server und seine Komponenten.
- Kapitel 2, „Einführung in den IBM SecureWay Boundary Server“ auf Seite 5, enthält Informationen über die Vorteile des SecureWay Boundary Server.
- Kapitel 3, „Vor der Installation von SecureWay Boundary Server“ auf Seite 13, enthält Informationen über die Planung des SecureWay Boundary Server.
- Kapitel 4, „Voraussetzungen für den IBM SecureWay Boundary Server (SBS)“ auf Seite 19, enthält Informationen über die Mindestvoraussetzungen für den SecureWay Boundary Server.
- In Kapitel 5, „SecureWay Boundary Server installieren und konfigurieren“ auf Seite 23, werden Installation und Konfiguration des SecureWay Boundary Server auf den Betriebssystemen Windows NT und AIX beschrieben.
- In Kapitel 6, „Referenzliteratur“ auf Seite 39, sind weitere Dokumentationen über den SecureWay Boundary Server und zugehörige Produkte aufgeführt.

Konventionen

In diesem Buch werden die folgenden Konventionen benutzt:

Konvention	Bedeutung
Fettdruck	Benutzerschnittstellenelemente wie Kontrollkästchen, Schaltflächen und Befehle.
Monospace-Schrift	Syntax- und Verzeichnisstandardwerte, die sich auf den SecureWay Boundary Server beziehen.
->	Steht für eine auszuwählende Folge von Menüoptionen. Beispiel: Wählen Sie **Datei-> Ausführen** aus. Dies bedeutet, daß erst auf **Datei** und dann auf **Ausführen** geklickt werden muß.

Web-Informationen

Informationen über die neuesten Änderungen an dem SecureWay Boundary Server sind unter der folgenden Web-Adresse verfügbar:

http://www.ibm.com/software/security/boundary/library

Informationen über Aktualisierungen an anderen IBM SecureWay FirstSecure-Produkten sind unter der folgenden Web-Adresse verfügbar:

http://www.ibm.com/software/security/firstsecure/library

Neue Einrichtungen und Funktionen

Version 2.0 von SecureWay Boundary Server enthält eine Vielzahl neuer Einrichtungen und Funktionen. Die wichtigsten neuen Einrichtungen und Funktionen sind nachfolgend aufgeführt.

Integration mit dem SecureWay Policy Director

Der SecureWay Policy Director kann Firewall-Proxy-Benutzer verwalten, wenn IBM Firewall für den SecureWay Boundary Server aktiviert ist. Firewall-Proxy-Benutzer werden für die folgenden Firewall-Services definiert:

- Telnet
- FTP
- HTTP
- Socks

Benutzer werden einschließlich der ihnen zugeordneten Richtlinien in einer LDAP-Datenbank (LDAP = Lightweight Directory Access Protocol) gespeichert.

Im SecureWay Directory bietet LDAP eine Möglichkeit zum Verwalten von Verzeichnisinformationen an einem zentralen Standort (Speichern, Aktualisieren, Abrufen und Datenaustausch). Der SecureWay Policy Director verwaltet Firewall-Proxy-Benutzer in der LDAP-Datenbank.

Optimierte Weiterleitung

Zur Optimierung der Weiterleitung wird ein SurfinGate-Plug-In der Finjan Software Ltd. benutzt, um den Datenaustausch auf dem Netz zum Filtern des Inhalts zu reduzieren.

Abwehren von Eindringlingen (Intrusion Blocking)

Über Befehlszeilenprogramme können in IBM Firewall dynamische Regeln zum Verweigern des Zugriffs erstellt werden. Das Abwehren von Eindringlingen kann in eine automatisierte Prozedur integriert werden.

IBM SecureWay Firewall 4.1

IBM SecureWay Firewall für Windows NT bietet folgendes:

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 4.1

IBM SecureWay Firewall für AIX bietet folgendes:

Erweiterte IPSec-Unterstützung

IBM SecureWay Firewall 4.1 beinhaltet erweiterte IPSec-Unterstützung einschließlich dreifache DES-Verschlüsselung und 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.

Symmetrischer Mehrprozessor (SMP)

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

Filtererweiterungen

Filter wurden erweitert und bieten eine bessere Leistung bei der Konfiguration. Sie können die Leistung von IBM Firewall optimieren, indem Sie die Position unterschiedlicher Arten von Filterregeln auswählen können. Zudem wird protokolliert, wie oft eine Verbindung benutzt wird.

Konfigurationsassistent

Ein Assistent ist bei der ersten Konfiguration von IBM SecureWay Firewall hilfreich. Durch diesen Konfigurationsassistenten können neue Benutzer nach der Installation von IBM Firewall schnell eine Firewall-Basiskonfiguration einrichten.

Network Security Auditor

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

Unterstützung in der Landessprache für Deutsch

Neben Brasilianisch, brasilianischem Portugiesisch, Englisch, Französisch, Italienisch, Japanisch, Koreanisch, vereinfachtem Chinesisch, Spanisch und traditionellem Chinesisch wird jetzt auch Deutsch unterstützt.

Netzadressenumsetzung

Die Netzadressenumsetzung wurde erweitert und unterstützt jetzt Viele-zu-Eins-Adressenzuordnungen. Bei dieser Zuordnung werden mehrere interne unregistrierte oder private Adressen über Anschlußnummern einer registrierten gültigen Adresse zugeordnet, um die eindeutigen Zuordnungen zu erstellen.

Von AIX und Windows NT unterstützte allgemeine Funktionen

Security Dynamics-ACE/Server

Der Security Dynamics-ACE/Server bietet zwei Authentifizierungsfaktoren. Diese Funktion wird erweitert und schützt das Netz und die Datenressourcen vor Eindringlingen, deren Aktionen (unabsichtlich oder absichtlich) zu Schäden führen können.

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 Benutzer-ID 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. Der Browser muß für die Benutzung eines HTTP-Proxy konfiguriert sein.

MIMEsweeper 2.0 für SecureWay

MIMEsweeper beinhaltet drei wichtige Komponenten: **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5** und **WEBsweeper 1.0_2**. Nachfolgend sind einige Erweiterungen aufgeführt.

MAILsweeper

MAILsweeper 4.1_2 für SMTP ist eine wichtige Erweiterung an dem Produkt MIMEsweeper der Content Technologies und bietet die folgenden neuen Einrichtungen:

- Eine benutzerfreundliche, hierarchische Richtlinienarchitektur bietet die Flexibilität zum Anwenden von Richtlinien auf der entsprechenden organisatorischen Stufe bis hin zu einzelnen Benutzern.
- Eine grafische Benutzerschnittstelle im Industriestandard vereinfacht das Konfigurieren von Software und das Erstellen und Verwalten von Richtlinien.
- Eine neue Einrichtung zum Aufteilen der Zustellung (Split Delivery) ist eine Funktion der hierarchischen Richtlinienimplementierung von Version 4. Bei Nachrichten mit mehreren Empfängern gelten für jeden einzelnen Empfänger individuelle Richtlinien. Berechtigte Empfänger erhalten die Nachricht, während unbefugten Empfängern die Nachrichtenzustellung verweigert wird.
- Durch die Multithreading-Nachrichtenverarbeitung wird der Durchsatz verbessert und die Zuverlässigkeit erhöht, da bei fehlerhaften Threads die Nachrichtenverarbeitung mit den restlichen Threads fortgesetzt werden kann.
- Zusammen mit Antivirusprodukten anderer Anbieter ermöglicht MAILsweeper das Erkennen und Entfernen von Viren in Nachrichten und Anlagen.
- Die erweiterte Textanalyse mit den Ausdrücken NEAR, AND, NOT und OR bietet eine enorme Flexibilität beim Erstellen benutzerfreundlicher, effektiver Szenarien auf der Basis der Nachrichtensyntax oder -architektur.
- Erweiterte Protokollierungs-Tools, die Daten an eine beliebige ODBC-konforme Datenbank senden können.
- Unterstützung des RBL-Servers (RBL = Real-Time Black List), der eine Liste mit Sites enthält, die für das Senden von Junk-E-Mail bekannt sind. MAILsweeper kann Anforderungen zum Einrichten von Verbindungen von Hosts zurückweisen, die in dieser Liste aufgeführt sind.
- Content Security ist durch attraktive Berichte, Grafiken und Tabellen über den E-Mail-Datenverkehr leichter zu verwalten.
- Integration mit LDAP-Verzeichnissen.
- Delivery Service Notification (DSN) unterstützt jetzt SNMP- und NT-Alerter.

WEBsweeper

- Durch zusätzliche Verbesserungen der Leistung wird die Datenverarbeitungsgeschwindigkeit erhöht.
- Es können Virenprüfprogramme für den HTTP- und FTP-Datenverkehr eingesetzt werden.

WEBsweeper HTTPS

- WEBsweeper bietet jetzt durch eine neue HTTPS-Proxy-Lösung vollständige Unterstützung für web-gestützte e-Commerce-Anwendungen.

SurfinGate 4.05

Zu den Erweiterungen an SurfinGate gehören:

Prüfung des JavaScript-Inhalts

SurfinGate 4.05 sucht nach möglicherweise problematischen JavaScript-Operationen und stoppt JavaScript-Code, der einen Konflikt mit den Sicherheitsrichtlinien des Unternehmens hervorruft. Mit SurfinGate 4.05 können Administratoren unternehmensweite Sicherheitsrichtlinien für JavaScript-, Java- und ActiveX-Codes, VisualBasic-Scripts und Cookies zentral verwalten, steuern und durchsetzen.

Aufgabenkritische Leistungsüberwachung

SurfinGate 4.05 enthält ein automatisches Tool, das ein abnormales Verhalten (beispielsweise Laufzeitfehler) erkennt und SurfinGate neu startet, falls ein Fehler auftritt. Dies ist eine wesentliche Sicherheitseinrichtung für aufgabenkritische Bereiche.

Verbesserte Richtlinienverwaltung

SurfinGate gibt unaufgelöste Minianwendungsprofile zum automatischen Blockieren in die Datenbank ein. Administratoren können die Liste der Minianwendungen/Steuerungen bearbeiten.

Unterstützung für die Protokolle FTP und SSL

SurfinGate 4.05 überwacht FTP-Kanäle auf mobilen Code und achtet auf Code, der andernfalls unbemerkt aus dem Internet eindringen könnte. Neben dem FTP-Datenverkehr überwacht SurfinGate auch den HTTP-Datenverkehr auf mobilen Code und leitet den HTTPS-Datenverkehr an zusätzliche Einheiten weiter.

Plug-In-Integration mit Firewall-HTTP-Proxy

SurfinGate arbeitet als Proxy in einer Proxy-Kette oder über ein Plug-In in WTE (Web Traffic Express) auf IBM Firewall für Windows NT.

Kapitel 1. Übersicht über den SecureWay Boundary Server

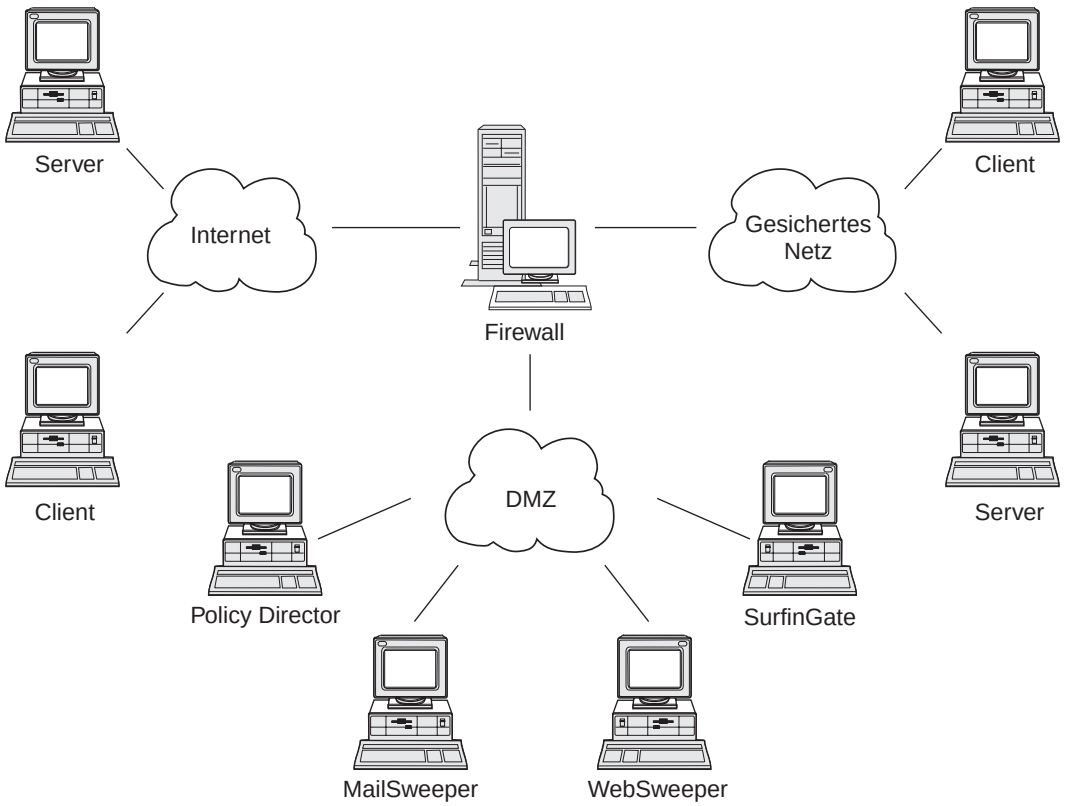

Abbildung 1. Beispiel für eine IBM SecureWay Boundary Server-Konfiguration

In diesem Beispiel benutzen fünf Workstations die Komponenten MAILsweeper, WEBsweeper, Policy Director und SurfinGate, um Web-Datenverkehr und Post zwischen Clients und Servern über eine Firewall zu überwachen und weiterzuleiten. In diesem Beispiel werden fünf physisch voneinander getrennte Workstations benutzt.

Beispiele für eine typische SecureWay Boundary Server-Konfiguration

Es wird empfohlen, die folgenden Maschinen für eine Mindestkonfiguration zu benutzen:

Tabelle 1. Hardwarevoraussetzungen für Boundary Server-Komponenten

Produkt	**Maschine**
IBM Firewall	Windows NT oder AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

Wollen Sie den SecureWay Boundary Server optimal nutzen, muß der SecureWay Policy Director im Netz vorhanden sein, damit Firewall-Proxy-Benutzer im SecureWay Directory (LDAP) gespeichert werden können.

Beispiel für HTTP (Windows NT-Firewall): In einem typischen Szenario geht eine HTTP-Anforderung für Internet-Inhalt von der Client-Maschine aus. Die Anforderung wird zuerst an WEBsweeper weitergeleitet. Auf dem Pfad für abgehende Anforderungen leitet WEBsweeper die Anforderung einfach an den Firewall-HTTP-Proxy weiter.

Am Firewall-HTTP-Proxy erfolgt die Authentifizierung des Benutzers. Bei der ersten Anforderung der Client-Sitzung für eine Suche im Internet wird zur Eingabe der Benutzer-ID und des Kennworts aufgefordert. Die Benutzer-ID wird zum Ermitteln der Client-Sicherheitsrichtlinien in der vom Policy Director verwalteten LDAP-Datenbank benutzt. Abhängig von den HTTP-Authentifizierungsrichtlinien für den Client und dem Ergebnis der Prüfung des eingegebenen Kennworts wird die Anforderung zurückgewiesen oder zugelassen. Für die Authentifizierungsoperation können weitere Zugriffe auf die LDAP-Datenbank oder den Security Dynamics ACE/Server erforderlich sein. Bei darauffolgenden Anforderungen dieser Sitzung für eine Suche im Internet liefert der Browser die Benutzer-ID und das Kennwort automatisch. Der Client wird zwar nicht zur Eingabe von Benutzer-ID und Kennwort aufgefordert, die Anforderung wird jedoch über denselben Prozeß wie bei der ersten Anforderung authentifiziert.

Ergibt die Authentifizierung, daß der Client die für die Anforderung erforderliche Berechtigung hat, wird die Anforderung an den entsprechenden Server im Internet weitergeleitet.

Kommt der Inhalt des Internet-Servers wieder am Firewall-HTTP-Proxy an, wird der Inhalt vom SurfinGate-Plug-In untersucht. Dem Plug-In werden für Richtlinienentscheidungen Gruppeninformationen für den Benutzer aus der LDAP-Datenbank zur Verfügung gestellt. Hat SurfinGate nichts am Inhalt auszusetzen, wird der Inhalt schnell und mit minimalem Verarbeitungsaufwand durch das Plug-In weitergeleitet. Inhalt mit JavaScript-Code wird im Plug-In gefiltert. Inhalt mit Java- oder ActiveX-Code wird zum Filtern an den SurfinGate-Server weitergeleitet und der gefilterte Inhalt an den Firewall-HTTP-Proxy zurückgegeben. Der Inhalt, der das Ergebnis der Verarbeitung durch das SurfinGate-Plug-In ist, wird an den WEBsweeper-Server zurückgesendet.

Wenn der Inhalt wieder am WEBsweeper-Server ankommt, wird er entsprechend der WEBsweeper-Richtlinien gefiltert und an den Client zurückgegeben.

Beispiel für HTTP (AIX-Firewall): Unter AIX ist der Fluß des Datenverkehrs weitgehend identisch, nur steht auf der AIX-Firewall kein SurfinGate-Plug-In zur Verfügung. Daher muß der SurfinGate-Server als Proxy in einer Proxy-Kette vom Client zur Firewall konfiguriert werden. WEBsweeper muß so konfiguriert werden, daß Anforderungen an den SurfinGate-Server und nicht direkt an den Firewall-HTTP-Proxy weitergeleitet werden. Der SurfinGate-Server muß dann so konfiguriert werden, daß Anforderungen an den Firewall-HTTP-Proxy weitergeleitet werden. Am SurfinGate-Server sind keine Gruppeninformationen verfügbar, daher können Richtlinienentscheidungen nur anhand der IP-Adresse getroffen werden.

Beispiel für Post: MAILsweeper wird als Post-Gateway konfiguriert. Der Inhalt der am MAILsweeper-Server ankommenden Post wird gefiltert, bevor er an den nächsten Post-Server weitergeleitet wird.

Alle gesicherten Post-Server müssen so konfiguriert sein, daß Client-Postanforderungen an den MAILsweeper-Server weitergeleitet werden. Der Firewall-Mail Exchanger muß so konfiguriert sein, daß ankommende Post an den MAILsweeper-Server weitergeleitet wird.

MAILsweeper muß so konfiguriert sein, daß die an eine beliebige externe Domäne adressierte Post an den Firewall-Mail Exchanger gesendet wird. MAILsweeper muß so konfiguriert sein, daß die an interne Domänen adressierte Post an den korrekten gesicherten Post-Server gesendet wird.

Kapitel 2. Einführung in den IBM SecureWay Boundary Server

Dieses Kapitel enthält eine Übersicht über den SecureWay Boundary Server und besteht aus folgenden Abschnitten:

Beschreibung des SecureWay Boundary Server

Der IBM SecureWay Boundary Server bietet die erste vollständige Lösung für die Sicherheit von Grenzen. Der SecureWay Boundary Server bietet Firewall-Schutz, den Betrieb virtueller privater Netze und Content Security. Der SecureWay Boundary Server kombiniert Technologien der Sicherheitsindustrie mit einer integrierten Lösung, die von IBM Unterstützung und Services flankiert wird. Zu dieser Lösung gehören:

- IBM SecureWay Firewall 4.1 (beinhaltet Security Dynamic ACE/Server)
- MIMEsweeper von Content Technologies
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS-Proxy 1.0_2
- SurfinGate 4.05 von Finjan
  - SurfinGate-Server
  - SurfinConsole
  - SurfinGate-Datenbank
  - SurfinGate-Plug-In für WTE-Integration für Windows NT 1.0

Vorteile des SecureWay Boundary Server

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, zwischen dem Netz oder den Anwendungen des Unternehmens und den Geschäftspartnern. Die Sicherheit von Grenzen schützt nicht nur Ihr Netz, Ihre Anwendungen und Informationen, sondern vergrößert auch deren Reichweite. Eine ordnungsgemäße Sicherheit von Grenzen setzt voraus, daß gesteuert wird, wer auf Ihr Netz zugreifen kann und welche Informationen in Ihr Netz gelangen oder Ihr Netz verlassen können.

Bedeutung von SecureWay Boundary Server in FirstSecure

IBM SecureWay FirstSecure ist ein Paket von integrierten Produkten und bietet ein benutzerfreundliches Gerüst zum Schutz des Netzbetriebs über das Internet und andere Netze. Es schützt Kundeninvestitionen durch ein modulares Design und miteinander kombinierbare Angebote und reduziert die Gesamtkosten für einen gesicherten e-business-Betrieb. Es bietet Virenschutz, Zugriffssteuerung, Steuerung des Datenverkehrsinhalts, Verschlüsselung, digitale Zertifikate, Firewall, Toolkits und Implementierungsservices.

Der Boundary Server ist ein Paket von Produkten zur Ergänzung von FirstSecure. Er erstellt eine Grenze zum Internet, durch die gefährliche Viren (über integrierte Virenprüfprogramme), JavaScript-Code, Java-Minianwendungen, ActiveX-Steuerungen und auch Junk-E-Mail (Spam) blockiert werden können. Mit dem Boundary Server kann genau gesteuert werden, welcher Internet-Inhalt in das eigene Netz gelangen darf. Mit dem SecureWay Policy Director werden Firewall-Proxy-Benutzer und ihre Authentifizierungsrichtlinien verwaltet.

Komponenten des SecureWay Boundary Server

Der SecureWay Boundary Server besteht aus den drei Komponenten IBM Firewall, MIMEsweeper und SurfinGate. Der SecureWay Boundary Server kann mit dem IBM SecureWay Policy Director integriert werden.

Übersicht über den IBM SecureWay Boundary Server

Der IBM SecureWay Boundary Server bietet großen Unternehmen die Voraussetzungen hinsichtlich des Zugriffsschutzes, der Zugriffssteuerung und der Content Security, die für die Ausnutzung des e-business durch eine sichere Öffnung ihrer Netze und Systeme für Kunden, Lieferanten und Geschäftspartner erforderlich sind. Zu den Einrichtungen gehören:

- Firewall-Schutz für das Netz.
- Betrieb eines virtuellen privaten Netzes (VPN) zur Vergrößerung der Reichweite des eigenen Netzes.
- Prüfprogramme für den Inhalt des E-Mail- und Web-Datenverkehrs, um die Daten des Unternehmens zu schützen, juristische Folgen zu begrenzen und die Produktivität aufrechtzuerhalten.

Der SecureWay Boundary Server kombiniert führende Technologie der Industrie mit einer integrierten Lösung, die von IBM Unterstützung und Services flankiert wird. Der SecureWay Boundary Server ist für die Betriebssysteme AIX und Windows NT verfügbar.

Funktionsweise von SecureWay Boundary Server

Der SecureWay Boundary Server schützt und verdeckt Ihr Netz und Ihre Systeme durch Paketfilterung, Proxies und Socks-Server-Technologie sowie Content Security. Durch diese Technologien können Administratoren explizit definieren, welche Daten in das Netz und aus dem Netz gelangen dürfen. Auf diese Weise werden Denial-of-Service-Attacken und das Eindringen von Hackern in das Netz verhindert. Zudem können mögliche juristische Folgen begrenzt werden. Der SecureWay Boundary Server bietet eine VPN-Lösung, damit Sie ferne Server und Modemgruppen durch eine Internet-gestützte Lösung ersetzen können.

Wird der SecureWay Boundary Server zusammen mit dem Policy Director genutzt, bietet er die Authentifizierung von Benutzern über ein zentrales richtliniengestütztes Schema. Als Schutz des Standorts gegen Viren kann mit dem SecureWay Boundary Server Antivirussoftware eingesetzt werden.

Übersicht über den IBM SecureWay Policy Director

Der Policy Director ist eine eigenständige Lösung für die Berechtigungs- und Sicherheitsverwaltung, die die Endpunkt-zu-Endpunkt-Sicherheit von Ressourcen über geografisch weit verstreute Intranets und Extranets bietet. Ein Extranet ist ein virtuelles privates Netz (VPN), das über Zugriffssteuerungs- und Sicherheitseinrichtungen die Benutzung von Intranets, die an das Internet angeschlossen sind, auf ausgewählte Subskribenten beschränkt. 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 und Extranets aufzubauen.

Funktionsweise von IBM SecureWay Policy Director

Wird der IBM SecureWay Policy Director zusammen mit dem SecureWay Boundary Server benutzt, bietet er das Speichern von Richtlinien und Authentifizierungsinformationen für Proxy-Benutzer.

Übersicht über IBM SecureWay Firewall

IBM SecureWay Firewall ist ein Programm für die Netzsicherheit. Eine Firewall ist eine Blockade zwischen gesicherten, internen, privaten Netzen und anderen Netzen oder dem Internet. Eine Firewall schützt vor unerwünschtem oder unbefugtem Datenverkehr in das und aus dem gesicherten Netz.

Funktionsweise von IBM SecureWay Firewall

IBM SecureWay Firewall schränkt den Zugriff zwischen einem geschützten Netz, dem Internet und anderen Gruppen von Netzen ein. Zudem sorgt IBM SecureWay Firewall für folgendes:

- Personen können nur an einem sorgfältig gesteuerten Punkt in das Netz gelangen.
- Attacken werden frühzeitig abgeblockt und gelangen nicht in die Nähe anderer Schutzeinrichtungen.
- Personen können nur an einem sorgfältig gesteuerten Punkt aus dem Netz gelangen.
- Interne Firewalls trennen sensible interne Informationen von unbefugten Mitarbeitern.
- Es kann festgelegt werden, welcher Datenverkehr in das Netz und aus dem Netz gelangen kann.

Übersicht über MIMEsweeper

MIMEsweeper bietet Content Security, indem der die Firewall durchlaufende E-Mail- oder Web-Datenverkehr analysiert wird. Durch Content Security können Unternehmen die durch die Benutzung von E-Mail und World Wide Web möglicherweise auftretenden Probleme lösen. Diese Probleme können in die Netzintegrität und die Geschäftsintegrität unterteilt werden.

Durch das Filtern zur Sicherung der Netzintegrität

- können Viren bei ankommender und abgehender E-Mail identifiziert und entfernt werden.
- können unerwünschte Dateitypen gefiltert werden.
- können zu große Dateien blockiert oder verzögert werden.
- können Netze gegen Überlastung oder Lahmlegung durch Mail-Bomb-Attacken geschützt werden.

Durch das Filtern zur Sicherung der Geschäftsintegrität

- können Verletzungen der Vertraulichkeit und der Verlust von Betriebsgeheimnissen verhindert werden.
- können mögliche juristische Folgen begrenzt werden.
- kann Produktivitätsverlust durch Mißbrauch von E-Mail- und World Wide Web-Services verringert werden.
- besteht Schutz gegen den Ausfall von Netzservices durch Mißbrauch und feindliche Attacken.

Gefahrenquellen für die Netzintegrität können zur Beschädigung oder zum Verlust von Daten, zur Unterbrechung des E-Mail-Flusses und zur Beschädigung von Systemhardware und damit zu Netzausfallzeiten, Produktivitätsverlusten und hohen Kosten für die Bereinigung und Wiederherstellung führen.

Gefahrenquellen für die Geschäftsintegrität können jedoch weit höheren Schaden anrichten, der zu enormen Kosten für Rechtsstreite, zum Verlust von gewerblichen Schutzrechten und zu einer Schädigung des Ansehens des Unternehmens führen kann. Probleme mit der Geschäftsintegrität können zu einem Stillstand der kommerziellen Operationen führen.

MIMEsweeper ist das führende Produkt zum Schutz von Unternehmen gegen Probleme mit der Netz- und Geschäftsintegrität, die durch die Nutzung von E-Mail und Internet in Unternehmen auftreten.

Funktionsweise von MIMEsweeper

MIMEsweeper kann

- abgehender Post rechtliche Ablehnungserklärungen hinzufügen.
- vertrauliche Dokumente und Daten schützen.
- E-Mail- und Web-Benutzer berechtigen und steuern.
- nicht der Netiquette entsprechendes Material isolieren oder blockieren.
- Junk-E-Mail blockieren.
- den Inhalt von Anlagen und heruntergeladenen Dateien überprüfen.
- Viren und heimtückischen Code stoppen.
- bestimmte unerwünschte Web-Seiten und -Sites blockieren.
- Berichte, Protokolle und Archive anlegen.

Übersicht über SurfinGate

SurfinGate 4.05 ist ein Sicherheits-Tool für mobilen Code für alle Geschäftstransaktionen, die über das Internet, Extranet oder Intranet ablaufen. Durch die Prüfung des Inhalts von mobilem Code (auch JavaScript-Code) hilft SurfinGate, Computernetze gegen beabsichtigte oder unbeabsichtigte Beschädigung zu schützen, beispielsweise gegen Industriespionage und das Verändern und Löschen von Informationen. SurfinGate überprüft den Inhalt von mobilem Java-, JavaScript- und ActiveX-Code auf Gateway-Ebene (hält solchen Code also von Ihren wichtigen Ressourcen fern) und ordnet dem Code eine eindeutige ID und ein Sicherheitsprofil für Minianwendungen (Applet Security Profile, ASP) zu, damit alle möglichen Sicherheitslücken erkannt werden. SurfinGate identifiziert Code, der möglicherweise problematisch ist, bereits bevor er das Netz gelangt.

SurfinGate 4.05 enthält vier Komponenten:

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

Der SurfinGate-Server agiert als HTTP-Proxy-Server. SurfinGate kann als Teil einer Proxy-Kette zusammen mit dem Firewall-HTTP-Proxy und dem WEBsweeper-Proxy plaziert werden. Für Windows NT kann SurfinGate alternativ als Plug-In für den Firewall-HTTP-Proxy benutzt werden. Bei der Benutzung als Plug-In erhält SurfinGate Gruppeninformationen über den Proxy-Benutzer, der die Anforderung vornimmt. Die SurfinGate-Richtlinien zum Filtern können auf diese Gruppeninformationen gestützt werden. Durch diese Architektur ist es möglich, Datenverkehr mit mobilem Code zu stoppen und zu überprüfen, bevor er Schaden anrichten kann. Diese Komponente bietet Schutz auf der Basis der Sicherheitsrichtlinien im Unternehmen.

SurfinConsole ist eine benutzerfreundliche Schnittstelle zum Verwalten und Einrichten zentraler Sicherheitsrichtlinien für mobilen Code im Unternehmen. 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. Die Datenbank kann eine eingebaute Datenbanksteuerkomponente für den Zugriff oder eine vorhandene Oracle-Datenbank verwenden. 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.

Funktionsweise von SurfinGate

SurfinGate bietet

- einen Server zur Prüfung des Inhalts von Java-Minianwendungen, JavaScript-Code und ActiveX-Steuerungen auf Gateway-Ebene.
- eine Überwachung in Echtzeit und dynamische Prüfung.
- die Durchsetzung der Sicherheitsrichtlinien für web-gestützten mobilen Code.
- die Prüfung von mobilem Code (beispielsweise Java-Minianwendungen, JavaScript-Code, ActiveX-Steuerungen, Visual Basic-Scripts, Plug-Ins, Cookies)

SurfinGate kann mit einem Proxy in einer Proxy-Kette oder über ein WTE-Plug-In auf IBM Firewall für Windows NT arbeiten.

Kapitel 3. Vor der Installation von SecureWay Boundary Server

In diesem Kapitel wird gezeigt, wie die Installation von SecureWay Boundary Server über den Assistenten vorbereitet werden kann. Es enthält die folgenden Abschnitte:

- „Vorbereitung“
- „SecureWay Boundary Server“ auf Seite 16

Vorbereitung

In diesem Abschnitt wird gezeigt, wie die Komponenten für den SecureWay Boundary Server vorbereitet werden.

Integration mit dem SecureWay Policy Director

Gehen Sie zum Einrichten einer IBM SecureWay Policy Director-Basiskonfiguration unter Windows NT oder AIX wie folgt vor:

1. Überprüfen Sie, ob das Betriebssystem so konfiguriert ist, daß der Policy Director unterstützt wird.
2. Stellen Sie fest, welche Server-Komponenten für Ihre Anforderungen am besten geeignet sind und auf welchen Maschinen diese Komponenten installiert werden sollen.
3. Installieren und konfigurieren Sie eine DCE-Infrastruktur, falls noch keine DCE-Infrastruktur besteht.
4. Installieren und konfigurieren Sie das SecureWay Directory (LDAP).
5. Konfigurieren Sie den Certificate Authorization Service (CAS), wenn die Client-Authentifizierung über Zertifikate erfolgen soll.
6. Installieren Sie den NetSEAT-Client.
7. Installieren Sie die Policy Director-Server-Komponenten.
8. Installieren Sie die Management Console.

Weitere Informationen über den Policy Director enthält das Buch *IBM SecureWay Policy Director Installation und Konfiguration 3.0*.

SecureWay Firewall

Gehen Sie zum Einrichten einer IBM Firewall-Basiskonfiguration unter Windows NT oder AIX wie folgt vor:

1. Achten Sie darauf, daß die in „Hardwarevoraussetzungen für den SecureWay Boundary Server“ auf Seite 19 aufgeführten Vorbedingungen erfüllt sind.
2. Planen Sie die IBM Firewall-Konfiguration. Legen Sie im voraus fest, welche Firewall-Funktionen Sie benutzen wollen und wie Sie die Funktionen benutzen wollen.
3. Teilen Sie der Firewall mit, welche ihrer Schnittstellen mit gesicherten Netzen verbunden sind. Damit die Firewall ordnungsgemäß funktioniert, muß sie über eine gesicherte Schnittstelle und eine ungesicherte Schnittstelle verfügen. Öffnen Sie über die Navigationsbaumstruktur des Konfigurations-Clients den Ordner **Systemverwaltung** und klicken Sie auf **Schnittstellen**, um eine Liste der Netzschnittstellen auf der Firewall aufzurufen. Wollen Sie den Sicherheitsstatus einer Schnittstelle ändern, wählen Sie eine Schnittstelle aus und klicken Sie auf **Ändern**.

   Anmerkung: Wollen Sie eine Verbindung zum Internet einrichten, nehmen Sie Kontakt mit Ihrem Internet Service Provider (ISP) auf und fordern Sie eine registrierte IP-Adresse für die ungesicherte Firewall-Schnittstelle an.
4. Konfigurieren Sie die allgemeinen Sicherheitsrichtlinien über die Anzeige **Sicherheitsrichtlinien** des Ordners **Systemverwaltung**. Typische Firewall-Konfigurationen sehen wie folgt aus:
   - DNS-Abfragen sind zugelassen
   - Rundsendenachrichten an ungesicherten Schnittstellen werden verweigert
   - Socks an ungesicherten Adaptern werden verweigert
5. Konfigurieren Sie den Domänennamensservice und die Postfunktion. Eine effiziente Kommunikation ist nur möglich, wenn eine DNS-Auflösung zur Verfügung gestellt wird. Greifen Sie über den Ordner **Systemverwaltung** der Navigationsbaumstruktur des Konfigurations-Clients auf diese Funktionen zu.
6. Definieren Sie Schlüsselelemente ihrer Netze über die Funktion **Netzobjekte** der Navigationsbaumstruktur des Konfigurations-Clients für die Firewall. Netzobjekte steuern den Datenverkehr durch die Firewall. Definieren Sie die folgenden Schlüsselelemente als Netzobjekte:
   - Gesicherte Schnittstelle der Firewall
   - Ungesicherte Schnittstelle der Firewall
   - Gesichertes Netz
   - Alle Teilnetze des gesicherten Netzes
   - Ein Host-Netzobjekt für die Security Dynamics-Server und die Windows NT-Domänen-Server (falls anwendbar)

7. Aktivieren Sie Services auf der Firewall. Dies sind die Methoden (beispielsweise Socks oder Proxy), über die Benutzer im gesicherten Netz auf das ungesicherte Netz zugreifen können. Welche Services implementiert werden, hängt von Entscheidungen ab, die Sie im Planungsstadium getroffen haben. Wird ein Service implementiert, müssen oft bestimmte Verbindungskonfigurationen eingerichtet werden, damit bestimmte Arten des Datenverkehrs erlaubt sind. Sollen beispielsweise gesicherte Benutzer über den HTTP-Proxy im Internet surfen dürfen, muß nicht nur der HTTP-Proxy-Dämon auf der Firewall konfiguriert werden, sondern es müssen auch Verbindungen eingerichtet werden, die den HTTP-Datenverkehr erlauben. Wollen Sie den Policy Director konfigurieren, können Sie weitere Informationen dem Abschnitt „Integration mit dem SecureWay Policy Director“ auf Seite 13 entnehmen.
8. **Nur Windows NT:** Da NetBIOS bei dem Prozeß zur Erhöhung der Netzsicherheit inaktiviert wird, wenn Sie Windows NT-Domänenkennwörter für die Authentifizierung benutzen wollen, müssen Sie den Windows-Client-Code konfigurieren, der die Fähigkeit zum Suchen von gesicherten Windows NT-Domänen zu Authentifizierungszwecken implementiert. Die gesicherten Windows NT-Server benötigen TCP/IP-Host-Namen und -Adressen sowie TCP/IP-Konnektivität zwischen ihnen und der Firewall. Der Firewall-Administrator muß Verbindungen zwischen der Firewall und den gesicherten Windows NT-Servern erstellen, damit der Datenverkehr zwischen Firewall und Servern ermöglicht wird.
9. Wird die Netzadressenumsetzung benutzt, nehmen Sie zunächst Kontakt zu Ihrem Internet Service Provider (ISP) auf und fordern Sie eine registrierte Internet-Adresse an, die für die Viele-zu-Eins-Adressenumsetzung benutzt werden soll. Diese Adresse ist zusätzlich zu der in Schritt 3 auf Seite 14 angeforderten Adresse erforderlich. Dann müssen Sie über die Anzeige *Konfiguration der NAT (Netzadressenumsetzung) hinzufügen* die registrierte Internet-Adresse als Viele-zu-Eins-IP-Adresse hinzufügen.

Anhand dieser Schritte können Sie eine Firewall-Basiskonfiguration einrichten. IBM Firewall verfügt über weitere Funktionen, beispielsweise über Systemprotokolle, die bei der Gewährleistung der Sicherheit des Netzes hilfreich sind.

Wird die Firewall normal oder abnormal abgeschaltet, gehen die Konfigurationsdaten nicht verloren, da sie auf der Festplatte gespeichert und beim Neustart automatisch wieder aktiviert werden. Es liegen jedoch bestimmte Firewall-Protokollnachrichten vor, in denen angegeben ist, daß bestimmte aktive Verbindungen unterbrochen wurden, beispielsweise eine aktive FTP-Sitzung.

SecureWay Boundary Server

IBM Firewall kann über den SecureWay Boundary Server-Assistenten so konfiguriert werden, daß IBM Firewall den IBM SecureWay Policy Director für die Benutzerverwaltung verwendet. Mit diesem Assistenten kann der Firewall-HTTP-Proxy auch für das Weiterleiten von Authentifizierungsinformationen an das SurfinGate-Plug-In konfiguriert werden (nur Windows NT).

Für die Konfiguration von IBM SecureWay Boundary Server für IBM Firewall sind folgende Informationen erforderlich:

- Der Host-Name und die Domäne des IBM SecureWay Directory-Servers, den die Firewall benutzen wird.
- Die Nummer des Anschlusses, auf dem der IBM SecureWay Directory-Server empfangsbereit ist. Der Standardanschluß ist 389.
- Das Sicherheitshauptkennwort für den IBM SecureWay Directory-Server.
- Der Domänenname, der zur Unterscheidung der Proxy-Benutzer für diese Firewall benutzt wird. Alle Firewalls, die diesen Namen verwenden, verwalten dieselbe Benutzergruppe. Normalerweise wird der vollständig qualifizierte Host-Name der Firewall-Maschine benutzt.
- Der Name des Firewall-Administrators, der für den Zugriff auf die im SecureWay Directory gespeicherten Proxy-Benutzer verwendet wird. Diesem Namen wird Zugriff zum Ändern aller im SecureWay Policy Director erstellten Proxy-Benutzer erteilt. Sie müssen den vollständig qualifizierten Host-Namen der Firewall-Maschine benutzen.
- Der registrierte Name, den das IBM SecureWay Directory als Stamm benutzt, von dem aus die Suche nach Firewall-Benutzern in der Datenbank gestartet wird. Dies muß das Suffix sein, das Sie in dem SecureWay Directory zum Speichern von Policy Director-Benutzern erstellt haben.
- Ein Kennwort für die Administrator-ID der Firewall, das bei der Verbindung zu dem IBM SecureWay Directory-Server benutzt wird.

Sie müssen eine Verbindung erstellen, damit Datenverkehr zwischen der Firewall und dem SecureWay Directory-Server fließen kann.

Achten Sie darauf, daß die in „Hardwarevoraussetzungen für den SecureWay Boundary Server“ auf Seite 19 aufgeführten Vorbedingungen erfüllt sind.

SurfinGate

Als Vorbereitung für die Benutzung von SurfinGate muß der Windows NT Service Pack 5 installiert werden. Achten Sie darauf, daß die in „Hardwarevoraussetzungen für den SecureWay Boundary Server“ auf Seite 19 aufgeführten Vorbedingungen erfüllt sind.

Gehen Sie wie folgt vor, um die Benutzung von SurfinGate vorzubereiten:

- Wenn Sie eine Oracle-Datenbank benutzen, muß sie konfiguriert werden.
- Wenn Sie Windows NT Firewall benutzen, müssen Sie entscheiden, ob Sie den Plug-In-Modus oder den Proxy-Modus verwenden.
- Installieren Sie zum Aktivieren des SurfinGate-Plug-Ins auf WTE das SurfinGate-Plug-In auf der Firewall-Maschine und rufen Sie den SecureWay Boundary Server-Assistenten auf.
- Sie müssen eine Verbindung erstellen, damit Datenverkehr zwischen dem SurfinGate-Plug-In und dem SurfinGate-Server fließen kann.

MIMEsweeper

Zur Vorbereitung der Benutzung von MIMEsweeper müssen Sie wissen, wie das Netz funktioniert. Achten Sie darauf, daß die in „Hardwarevoraussetzungen für den SecureWay Boundary Server“ auf Seite 19 aufgeführten Vorbedingungen erfüllt sind.

MAILsweeper

Wenn Sie MIMEsweeper konfigurieren, müssen sich MAILsweeper und WEBsweeper auf separaten Maschinen befinden.

Führen Sie die folgenden Aufgaben aus, bevor Sie MAILsweeper konfigurieren:

- Legen Sie die Postdomänen fest, die Sie intern benutzen. MAILsweeper und der Firewall-Mail Exchanger müssen so konfiguriert sein, daß Post für jede dieser Postdomänen akzeptiert wird.
- Legen Sie fest, welche gesicherten Post-Server die einzelnen Domänen unterstützen. MAILsweeper muß so konfiguriert sein, daß an eine Postdomäne adressierte Post an den korrekten gesicherten Post-Server weitergeleitet wird.
- Legen Sie die Adresse des MAILsweeper-Servers fest. Alle gesicherten Post-Server müssen so konfiguriert sein, daß die von internen Clients empfangene Post an den MAILsweeper-Server weitergeleitet wird.
- Legen Sie die Adresse der Firewall fest. MAILsweeper muß so konfiguriert sein, daß die an externe Domänen adressierte Post an den Firewall-Mail Exchanger weitergeleitet wird.

WEBsweeper

Führen Sie die folgenden Aufgaben aus, bevor Sie WEBsweeper konfigurieren:

- Legen Sie die Adresse des WEBsweeper-Servers fest. Diese Adresse wird von allen Client-Web-Browsern im Netz benötigt. Die Browser müssen so konfiguriert sein, daß der WEBsweeper-Server als Proxy für HTTP, FTP und HTTPS benutzt wird.
- Legen Sie die Adresse der gesicherten Schnittstelle der Firewall fest. WEBsweeper muß so konfiguriert sein, daß Proxy-Anforderungen an den HTTP-Proxy auf der Firewall weitergeleitet werden.
- Wollen Sie verhindern, daß Clients das Filtern des Web-Inhalts umgehen können, müssen Sie eine Verbindung auf der Firewall einrichten, um den Proxy-Zugriff auf die WEBsweeper- und/oder SurfinGate-Server zu begrenzen.

Kapitel 4. Voraussetzungen für den IBM SecureWay Boundary Server (SBS)

In diesem Kapitel sind die Mindestvoraussetzungen für den SecureWay Boundary Server aufgeführt.

Hardwarevoraussetzungen für den SecureWay Boundary Server

In der folgenden Tabelle sind die Hardwarevoraussetzungen für die Boundary Server-Komponenten aufgeführt.

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

Boundary Server-Komponente	Maschinentyp	Plattenspeicherplatz	Hauptspeicher	Weitere Voraussetzungen
Policy Director	-	64 MB	16 MB	-
IBM Firewall	Windows NT: 266 MHz oder höher AIX: RS/6000-Maschine, die AIX 4.3.2 unterstützt	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	2 Netzschnittstellenkarten
ACE/Server	Windows NT: 166 MHz oder höher (nur Einzelprozessor) 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 2 (Seite 2 von 2). Hardwarevoraussetzungen für die Boundary Server-Komponenten				
MAILsweeper	Windows NT: 400 MHz-Prozessor oder höher	1 GB	128 MB	-
WEBsweeper	Windows NT: 450 MHz-Prozessor oder höher	1 GB	128 MB	-
WEBsweeper-Systemvoraus-setzungen für eine Umgebung mit hohem Volumen	Windows NT: 450 MHz-Prozessor oder höher	3 GB	512 MB	-
SurfinGate 4.05 Server	Windows NT: 233 MHz-Prozessor oder höher	20 MB	256 MB	-
SurfinGate 4.05 Console	Windows NT: 233 MHz-Prozessor oder höher	15 MB	64 MB	-

Anmerkung: Weitere Informationen enthält das Buch *IBM SecureWay Firewall for AIX or Windows NT Version Setup and Installation for Multiple Languages*. Zudem sind 138 MB Plattenspeicherplatz für den Netscape-Browser erforderlich.

Softwarevoraussetzungen für den SecureWay Boundary Server

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

Tabelle 3. Mindestsoftwarevoraussetzungen für die Boundary Server-Komponenten

Produkt	Windows	AIX	Weitere Voraussetzungen
Policy Director-Server	Windows NT Version 4.0 mit Service Pack 5	4.3.1	-
IBM Firewall	Windows NT Version 4.0 mit Service Pack 5	4.3.2	-
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	-
MAILsweeper	Windows NT Version 4.0 mit Service Pack 5, Internet Explorer 4.01 oder höher, Microsoft Management Console 1.1, NTFS-Laufwerk, Windows Messaging	-	Die gewünschten Antivirus-Tools
WEBsweeper	Windows NT Version 4.0 mit Service Pack 5	-	Die gewünschten Antivirus-Tools
SurfinGate Server	Windows NT Version 4.0 mit Service Pack 5	-	-
SurfinGate 4.05 Console	Windows NT Version 4.0 mit Service Pack 5 oder Windows 95	-	-

Kapitel 5. SecureWay Boundary Server installieren und konfigurieren

In diesem Kapitel wird gezeigt, wie der SecureWay Boundary Server unter Windows NT und AIX konfiguriert und installiert wird. Das Kapitel besteht aus folgenden Abschnitten:

- „SecureWay Boundary Server-Komponenten installieren“
- „SecureWay Boundary Server-Komponenten konfigurieren“ auf Seite 26
- „Abwehren von Eindringlingen“ auf Seite 35

SecureWay Boundary Server-Komponenten installieren

Dieser Abschnitt dient als Hilfe bei der Installation von IBM SecureWay Firewall, SurfinGate und MIMEsweeper für Windows NT und AIX.

SecureWay Firewall installieren

Weitere Informationen über eine Basiskonfiguration für IBM SecureWay Firewall für Windows NT und AIX enthält der Abschnitt „Vorbereitung“ auf Seite 13. In diesem Abschnitt wird gezeigt, wie eine sichere Schnittstelle definiert wird, die Sicherheitsrichtlinien festgelegt und Netzobjekte definiert werden. Weitere Informationen über die Installation von SecureWay Firewall enthalten die Bücher *IBM SecureWay Firewall für AIX Konfiguration und Installation* und *IBM SecureWay Firewall für Windows NT Konfiguration und Installation*.

SecureWay Directory installieren

Wird die LDAP-Funktion von SecureWay Boundary Server benutzt, muß das SecureWay Directory installiert werden. Weitere Informationen enthält das Buch *IBM SecureWay Policy Director Installation und Konfiguration 3.0*.

Der SecureWay Directory-Server muß sich auf der gesicherten Seite der Firewall oder innerhalb der DMZ (Demilitarized Zone) der Firewall befinden.

SecureWay Policy Director installieren

Wird die LDAP-Funktion von SecureWay Boundary Server benutzt, muß der SecureWay Policy Director installiert werden. Weitere Informationen enthält das Buch *IBM SecureWay Policy Director Installation und Konfiguration 3.0*.

SecureWay Boundary Server installieren

Gehen Sie wie folgt vor, um den SecureWay Boundary Server unter Windows NT zu installieren:

- Installieren Sie SecureWay Firewall für Windows NT.
- Führen Sie auf der SecureWay Boundary Server-CD die Datei setup.exe aus.
- Wählen Sie die gewünschte Sprache und klicken Sie auf **OK**.
- InstallShield fragt nach, wo der SecureWay Boundary Server installiert werden soll. Das Windows NT-Standardverzeichnis ist C:\Program Files\IBM\SBS.
- Starten Sie das System neu.

Gehen Sie wie folgt vor, um den SecureWay Boundary Server unter AIX zu installieren:

- Installieren Sie SecureWay Firewall für AIX.
- Legen Sie die CD ein und führen Sie die Installation über SMITTY aus.
- Wählen Sie **Softwareinstallation und Wartung** aus.
- Wählen Sie **Software installieren und aktualisieren** aus.
- Wählen Sie **Neueste verfügbare Software installieren und aktualisieren** aus.
- Wenn Sie nach der Eingabeeinheit gefragt werden, wählen Sie das CD-ROM-Laufwerk aus.
- Wählen Sie aus der Liste der installierbaren Software `sbs` aus.
- Drücken Sie die Eingabetaste, um die Software zu installieren.
- Starten Sie das System neu.

SurfinGate installieren

Zu SurfinGate gehören die beiden Komponenten SurfinGate Server und SurfinGate Console. Wollen Sie eine dieser SurfinGate-Komponenten installieren, können Sie weitere Informationen dem Installationsbuch entnehmen. Dieses Buch befindet sich auf der SurfinGate-CD in der Datei `\docs\install.pdf`.

SurfinGate-Plug-In

Wollen Sie das SurfinGate-Plug-In für IBM SecureWay Firewall für Windows NT installieren, können Sie weitere Informationen dem Installationsbuch entnehmen. Dieses Buch befindet sich im Verzeichnis `\docs` auf der SurfinGate-CD.

MIMEsweeper installieren

Zu MIMEsweeper gehören die drei Komponenten MAILsweeper, WEBsweeper und WEBsweeper HTTPS.

MAILsweeper 4.1 muß auf einer NTFS-Partition installiert werden.

MAILsweeper installieren

Informationen über die Installation von MAILsweeper enthält das Buch *Getting Started Guide*, das sich in der Datei `\install\MSW4_0_2\docs\qsg.pdf` auf der MIMEsweeper-CD befindet.

Installieren Sie MAILsweeper **NICHT** auf derselben Maschine wie den WEBsweeper-HTTP-Proxy.

Installieren Sie MAILsweeper **NICHT** auf derselben Maschine wie den WEBsweeper HTTPS-Proxy.

Wenn Sie die Datei `MAPI32.dll` von der Windows NT-CD und dann die Microsoft Management Console 1.1 von der MIMEsweeper-CD installieren, wird die korrekte Version der Datei `MAPI32.dll` durch eine frühere Version überschrieben, die mit der Microsoft Management Console installiert wird. Achten Sie darauf, daß Sie nach der Installation der Microsoft Management Console die Datei `MAPI32.dll` mit Version 4.0 oder höher installieren. Die `dll` befindet sich normalerweise in der Komponente Windows Messaging.

WEBsweeper installieren

Informationen über die Installation von WEBsweeper enthält das Buch *Administrator's Guide*, das sich in der Datei `\install\WSW3_2_5\docs\manual.pdf` auf der MIMEsweeper-CD befindet.

Installieren Sie WEBsweeper **NICHT** auf derselben Maschine wie MAILsweeper.

WEBsweeper HTTPS installieren

Informationen über die Installation von WEBsweeper HTTPS enthält die Informationsdatei *Readme* in der Datei `\install\WSWHTTPS1_0_2\readme.txt` auf der MIMEsweeper-CD.

Installieren Sie den WEBsweeper HTTPS-Proxy **NICHT** auf derselben Maschine wie MAILsweeper.

SecureWay Boundary Server-Komponenten konfigurieren

SecureWay Firewall konfigurieren

Gehen Sie wie folgt vor, um eine IBM Firewall-Basiskonfiguration einzurichten:

1. Planen Sie die IBM Firewall-Konfiguration. Legen Sie im voraus fest, welche Firewall-Funktionen Sie benutzen wollen und wie Sie die Funktionen benutzen wollen.
2. Teilen Sie der Firewall mit, welche ihrer Schnittstellen mit gesicherten Netzen verbunden sind. Damit die Firewall ordnungsgemäß funktioniert, muß sie über eine gesicherte Schnittstelle und eine ungesicherte Schnittstelle verfügen. Öffnen Sie über die Navigationsbaumstruktur des Konfigurations-Clients den Ordner **Systemverwaltung** und klicken Sie auf **Schnittstellen**, um eine Liste der Netzschnittstellen auf der Firewall aufzurufen. Wollen Sie den Sicherheitsstatus einer Schnittstelle ändern, wählen Sie eine Schnittstelle aus und klicken Sie auf **Ändern**.
3. Konfigurieren Sie die allgemeinen Sicherheitsrichtlinien über die Anzeige **Sicherheitsrichtlinien** des Ordners **Systemverwaltung**. Typische Firewall-Konfigurationen sehen wie folgt aus:
   - DNS-Abfragen sind zugelassen
   - Rundsendenachrichten an ungesicherten Schnittstellen werden verweigert
   - Socks an ungesicherten Adaptern werden verweigert
4. Konfigurieren Sie den Domänennamensservice und die Postfunktion. Eine effiziente Kommunikation ist nur möglich, wenn eine DNS-Auflösung zur Verfügung gestellt wird. Greifen Sie über den Ordner **Systemverwaltung** der Navigationsbaumstruktur des Konfigurations-Clients auf diese Funktionen zu.
5. Definieren Sie Schlüsselelemente ihres Netzes für die Firewall über die Funktion **Netzobjekte** in der Navigationsbaumstruktur des Konfigurations-Clients. Netzobjekte steuern den Datenverkehr über die Firewall. Definieren Sie die folgenden Schlüsselelemente als Netzobjekte:
   - Gesicherte Schnittstelle der Firewall
   - Ungesicherte Schnittstelle der Firewall
   - Gesichertes Netz
   - Alle Teilnetze des gesicherten Netzes
   - Ein Host-Netzobjekt für die Security Dynamics-Server und die Windows NT-Domänen-Server (falls anwendbar)

6. Aktivieren Sie Services auf der Firewall. Dies sind die Methoden, über die Benutzer im gesicherten Netz auf das ungesicherte Netz zugreifen können (beispielsweise Socks oder Proxy). Welche Services implementiert werden, hängt von den Entscheidungen ab, die Sie im Planungsstadium getroffen haben. Wird ein Service implementiert, müssen oft bestimmte Verbindungskonfigurationen eingerichtet werden, damit bestimmte Arten des Datenverkehrs erlaubt sind. Sollen beispielsweise gesicherte Benutzer über den HTTP-Proxy im Internet surfen dürfen, muß nicht nur der HTTP-Proxy-Dämon auf der Firewall konfiguriert werden, sondern es müssen auch Verbindungen eingerichtet werden, die den HTTP-Datenverkehr erlauben.
7. Definieren Sie Firewall-Benutzer. Ist für Funktionen wie abgehende Web-Zugriffe oder für Firewall-Administratoren eine Authentifizierung erforderlich, müssen Sie diese Benutzer für die Firewall definieren. Wenn Sie den SecureWay Policy Director benutzen, um Proxy-Benutzer im LDAP zu speichern, erstellen Sie jetzt noch keine Proxy-Benutzer. Erstellen Sie Firewall-Proxy-Benutzer während der Policy Director-Konfiguration über die Policy Director-Konsole.

Anhand dieser Schritte können Sie eine Firewall-Basiskonfiguration einrichten. IBM Firewall verfügt über weitere Funktionen, beispielsweise über Systemprotokolle, die bei der Gewährleistung der Sicherheit des Netzes hilfreich sind.

Wird die Firewall normal oder abnormal abgeschaltet, gehen die Konfigurationsdaten nicht verloren, da sie auf der Festplatte gespeichert und beim Neustart automatisch wieder aktiviert werden. Es können jedoch bestimmte Firewall-Protokollnachrichten vorliegen, in denen angegeben ist, daß bestimmte aktive Verbindungen unterbrochen wurden, beispielsweise eine aktive FTP-Sitzung.

SecureWay Firewall für die Integration von Policy Director konfigurieren

Die Firewall muß über den SecureWay Boundary Server-Assistenten so konfiguriert werden, daß sie den IBM SecureWay Policy Director benutzt, damit die Policy Director-Integration genutzt werden kann. Wird der IBM SecureWay Policy Director nicht benutzt, werden Proxy-Benutzer nur über die grafische Firewall-Benutzerschnittstelle definiert. Solche Benutzer können nicht mit dem SecureWay Policy Director verwaltet werden.

Es muß eine Verbindung eingerichtet werden, damit SecureWay Firewall mit dem SecureWay Directory kommunizieren kann. Das SecureWay Directory muß sich auf der gesicherten Seite der Firewall befinden (gesicherte DMZ oder gesichertes Netz).

Weitere Informationen über die Einrichtung von Verbindungen enthalten die Bücher *IBM SecureWay Firewall für Windows NT Benutzerhandbuch* und *IBM SecureWay Firewall für AIX Benutzerhandbuch*. Es folgen Informationen zur Einrichtung der Verbindung.

Für die Anforderung müssen die Regeln für abgehende Verbindungen wie folgt konfiguriert werden:

- Die Quellenadresse ist die Adresse des gesicherten Firewall-Adapters.
- Die Zieladresse ist die SecureWay Directory-Adresse.
- Der Quellenanschluß ist größer als 1023.
- Der Zielanschluß ist gleich 389.
- Die Schnittstelle ist gesichert.
- Die Weiterleitung erfolgt lokal.
- Die Richtung ist abgehend.

Für die Antwort müssen die Regeln für ankommende Verbindungen wie folgt konfiguriert werden:

- Die Quellenadresse ist die SecureWay Directory-Adresse.
- Die Zieladresse ist die Adresse des gesicherten Firewall-Adapters.
- Der Quellenanschluß ist gleich 389.
- Der Zielanschluß ist größer als 1023.
- Die Schnittstelle ist gesichert.
- Die Weiterleitung erfolgt lokal.
- Die Richtung ist ankommend.

Nachfolgend wird ein Beispiel für eine solche Verbindung gezeigt:

```
# Service : ldap
# Description :

permit 9.67.130.153 255.255.255.255 9.67.141.85
255.255.255.255 tcp gt 1023 eq 389 secure both
outbound l=y f=y t=0 e=none a=none

permit 9.67.141.85 255.255.255.255 9.67.130.153
255.255.255.255 tcp/ack eq 389 gt 1023 secure local
inbound l=y f=y t=0 e=none a=none
```

Rufen Sie den SecureWay Boundary Server-Konfigurationsassistenten auf. Wählen Sie die Option zum Aktivieren der Zusammenarbeit von Firewall und Policy Director aus. Weitere Informationen enthält „SecureWay Boundary Server für Policy Director-Integration konfigurieren“ auf Seite 31.

SecureWay Firewall für die Benutzung von SurfinGate-Plug-Ins konfigurieren (nur Windows NT)

Es muß eine Verbindung eingerichtet werden, damit SecureWay Firewall mit dem SurfinGate-Server kommunizieren kann. Der SurfinGate-Server muß sich auf der gesicherten Seite der Firewall befinden.

Weitere Informationen über die Einrichtung von Verbindungen enthält das Buch *IBM SecureWay Firewall für Windows NT Benutzerhandbuch*. Es folgen Informationen zur Einrichtung der Verbindung.

Für die Anforderung müssen die Regeln für abgehende Verbindungen wie folgt konfiguriert werden:

- Die Quellenadresse ist die Adresse des gesicherten Firewall-Adapters.
- Die Zieladresse ist die Adresse des SurfinGate-Servers.
- Der Quellenanschluß ist größer als 1023.
- Der Zielanschluß ist gleich 3141.
- Die Schnittstelle ist gesichert.
- Die Weiterleitung erfolgt lokal.
- Die Richtung ist abgehend.

Für die Anforderung müssen die Regeln für ankommende Verbindungen wie folgt konfiguriert werden:

- Die Quellenadresse ist die Adresse des SurfinGate-Servers.
- Die Zieladresse ist die Adresse des gesicherten Firewall-Adapters.
- Der Quellenanschluß ist gleich 3141.
- Der Zielanschluß ist größer als 1023.
- Die Schnittstelle ist gesichert.
- Die Weiterleitung erfolgt lokal.
- Die Richtung ist ankommend.

Nachfolgend wird ein Beispiel für eine solche Verbindung gezeigt:

```
# Service : SurfinGate Plugin Communication
# Description:

permit 9.67.143.113 255.255.255.255 9.67.143.115 255.255.255.255 tcp gt 1023 eq 3141
secure local outbound l=y f=y
permit 9.67.143.115 255.255.255.255 9.67.143.113 255.255.255.255 tcp eq 3141 gt 1023
secure local inbound  l=y f=y

Anmerkung: Die Verbindungen müssen über dieselbe Leitung erfolgen.
```

Sie müssen zudem den SurfinGate-Server so konfigurieren, daß die Daten durchsucht werden können. In der SurfinConsole (der Verwaltungsschnittstelle von SurfinGate) müssen Sie die Option **Plugin Mode** der Registerkarte **General** markieren. Zudem müssen Sie die Adresse und Anschlußnummer des Firewall-HTTP-Proxy in das Feld **Next Proxy** der Registerkarte **Proxy** eingeben.

SecureWay Firewall für die Benutzung von MAILsweeper konfigurieren

Der in SecureWay Firewall definierte Mail Exchanger muß auf die MAILsweeper-Maschine und nicht auf den aktuellen gesicherten Post-Server zeigen. MAILsweeper selbst leitet Post an die gesicherten Post-Server weiter.

SecureWay Policy Director konfigurieren

Überprüfen Sie, ob das SecureWay Directory installiert wurde. Sie müssen wissen, welche Adresse die Maschine hat, auf der das SecureWay Directory installiert ist, auf welchem Anschluß das SecureWay Directory empfangsbereit ist, welche Administrator-ID dem SecureWay Directory-Server zugeordnet ist und wie das Administratorkennwort lautet.

Installieren Sie den SecureWay Directory-LDAP-Client auf derselben Maschine wie den SecureWay Policy Director. (Der Client kann bereits installiert sein, wenn Sie für das SecureWay Directory und den SecureWay Policy Director dieselbe Maschine benutzen.)

Sie müssen das LDAP-Schema des SecureWay Directory ändern, wenn Policy Director-eProxy-Benutzer unterstützt werden sollen. Die am Schema vorgenommenen Hinzufügungen werden in zwei vom Policy Director zur Verfügung gestellten Dateien gespeichert. Sie benötigen die Dateien `secschema.def` und `puschema.def`, die sich im Verzeichnis `/schema` der Policy Director-CD befinden.

Geben Sie auf der Policy Director-Maschine die folgenden Befehle ein, um das LDAP-Schema auf dem SecureWay Directory-Server zu ändern:

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMBENID> -w <LDAPADMKW> -f secschema.def

ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMBENID> -w <LDAPADMKW> -f puschema.def
```

Dabei gilt folgendes:

- `<LDAPHOST>` ist der SecureWay Directory-Server-Name
- `<LDAPPORT>` ist der Anschluß, auf dem der Server empfangsbereit ist
- `<LDAPADMBENID>` ist die Administrator-ID
- `<LDAPADMKW>` ist das Administratorkennwort

Haben Sie das LDAP-Schema für die Unterstützung von Proxy-Benutzern geändert, müssen Sie die Bearbeitung von Proxy-Benutzern für die Policy Director Console aktivieren. Hierzu müssen Sie die Kommentarzeichen in der Zeile `Proxyusers TaskView` der Datei `console.properties` entfernen. Diese Datei befindet sich im Verzeichnis `\Program Files\IBM\IVConsole`.

SecureWay Directory konfigurieren

Für das SecureWay Directory muß ein Suffix definiert werden, das als Stamm zum Speichern von Policy Director-Benutzern verwendet werden soll. Im Buch *IBM SecureWay Directory Administrator's Guide* wird gezeigt, wie LDAP ein Suffix hinzugefügt wird. Ein typisches Suffix kann beispielsweise wie folgt aussehen:

```
o=yourcompany,c=yourcountry
```

Haben Sie das Suffix zum Speichern von Policy Director-Benutzern hinzugefügt, müssen sie seine Zugriffssteuerungsliste (Access Control List, ACL) korrekt festlegen. Sie müssen dem neuen Suffix alle Zugriffsrechte für die Policy Director-Sicherheitsgruppe liefern. Der registrierte Name (Distinguished Name, DN) für die Policy Director-Sicherheitsgruppe lautet:

```
cn=securitygroup,secauthority=default
```

SecureWay Boundary Server für Policy Director-Integration konfigurieren

Der SecureWay Boundary Server kann über den Assistenten konfiguriert werden. Dieser Assistent führt durch die Schritte, die erforderlich sind, um die Firewall für die Zusammenarbeit mit anderen Produkten im Boundary Server und Policy Director zu konfigurieren. In den Anzeigen werden Fragen über den LDAP-Server gestellt. Haben Sie alle erforderlichen Informationen eingegeben, konfiguriert der Assistent die Firewall so, daß sie die LDAP-Datenbank benutzt, die auch der Policy Director für Benutzer- und Gruppenrichtlinien verwendet. Mit diesem Assistenten kann der Firewall-HTTP-Proxy auch für das Weiterleiten von Authentifizierungsinformationen an das SurfinGate-Plug-In konfiguriert werden (nur Windows NT-Firewall). Der Assistent kann diese Konfiguration auch wieder entfernen.

Rufen Sie den SecureWay Boundary Server-Assistenten auf, wenn Sie den IBM SecureWay Boundary Server konfigurieren wollen. Geben Sie unter AIX den Befehl **sbswizard** ein. Wählen Sie unter Windows NT **Start->Programme->SecureWay Boundary Server** aus. Daraufhin wird der SecureWay Boundary Server-Assistent aufgerufen.

1. Wählen Sie die Option **Firewall für eine gemeinsame Benutzung einer LDAP-Datenbank mit dem Policy Director konfigurieren** aus.
2. Beantworten Sie die gestellten Fragen anhand der Informationen in „SecureWay Boundary Server“ auf Seite 16.

SecureWay Boundary Server zur Aktivierung des SurfinGate-Plug-Ins konfigurieren (nur Windows NT)

Wählen Sie **Start->Programme->SecureWay Boundary Server** aus. Daraufhin wird der SecureWay Boundary Server-Assistent aufgerufen.

1. Wählen Sie die Option **Firewall-HTTP-Proxy so konfigurieren, daß Informationen zur Identifikationsüberprüfung an das SurfinGate-Plug-In übergeben werden** aus.
2. Beenden Sie den Dialog.

SurfinGate konfigurieren

Unter Windows NT kann SurfinGate auf zwei Arten konfiguriert werden:

- Als verketteter Proxy
- Als Plug-In für den Firewall-HTTP-Proxy

Unter AIX kann SurfinGate nur auf eine einzige Art konfiguriert werden:

- Als verketteter Proxy

SurfinGate als verketteten Proxy konfigurieren

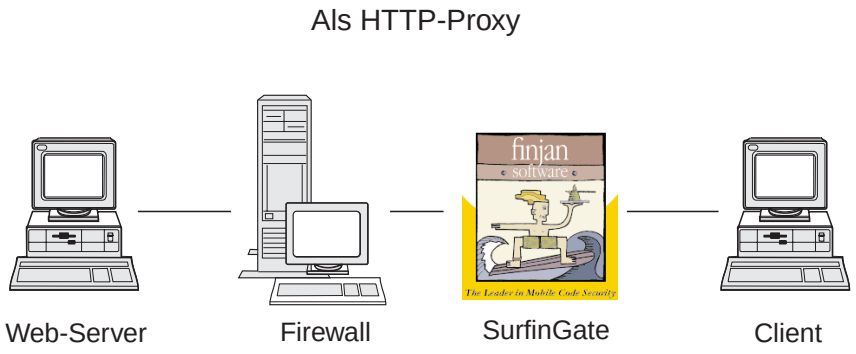

Abbildung 2. SurfinGate-Konfigurationen

Die Client-Web-Browser müssen so konfiguriert sein, daß SurfinGate als Proxy für HTTP, FTP und HTTPS benutzt wird. Achten Sie darauf, daß Sie die Nummer des Anschlusses angeben, auf dem SurfinGate empfangsbereit ist (der Standardwert ist 8080). In der SurfinConsole (der Verwaltungsschnittstelle von SurfinGate) müssen Sie die Option **Proxy Mode** der Registerkarte **General** markieren. Zudem müssen Sie die Adresse und Anschlußnummer des Firewall-HTTP-Proxy in das Feld **Next Proxy** der Registerkarte **Proxy** eingeben. Als Alternative können Sie, wenn bereits weitere Proxies definiert sind, auf diese Proxies als nächsten Proxy zeigen.

SurfinGate als Plug-In für den Firewall-HTTP-Proxy konfigurieren

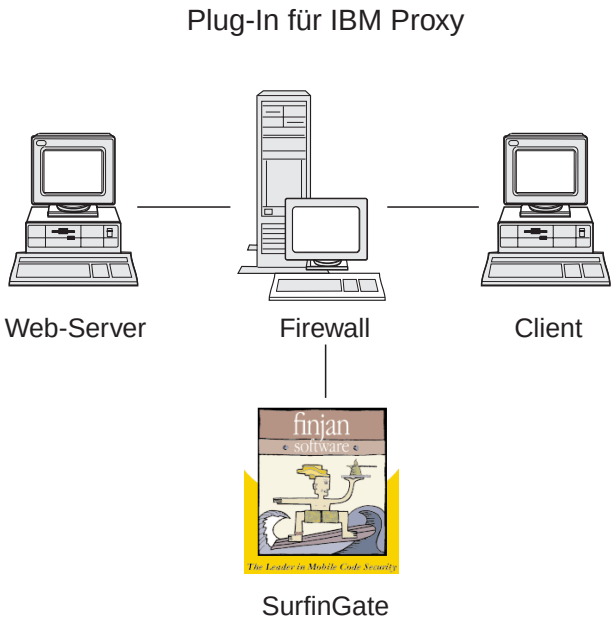

Abbildung 3. SurfinGate-Konfigurationen

Die Client-Web-Browser müssen so konfiguriert sein, daß der Firewall-HTTP-Proxy als Proxy für HTTP, FTP und HTTPS benutzt wird. Geben Sie die Nummer des Anschlusses an, auf dem der Firewall-HTTP-Proxy empfangsbereit ist (der Standardwert ist 8080).

In der SurfinConsole (der Verwaltungsschnittstelle von SurfinGate) müssen Sie die Option **Plugin Mode** der Registerkarte **General** markieren. Zudem müssen Sie die Adresse und Anschlußnummer des Firewall-HTTP-Proxy in das Feld **Next Proxy** der Registerkarte **Proxy** eingeben.

Anmerkung: Diese Funktionalität ist nur auf IBM SecureWay Firewall für Windows NT verfügbar.

MIMEsweeper konfigurieren

MAILsweeper konfigurieren

Abbildung 4. MAILsweeper-Konfigurationen

In einer einfachen Umgebung muß MAILsweeper anhand der während der Installation gestellten Fragen konfiguriert werden. Wollen Sie weitere Konfigurationsaufgaben ausführen, wählen Sie **Start->Programme->MAILsweeper for SMTP->MAILsweeper for SMTP Console** aus. Weitere Informationen enthält das Buch *MAILsweeper Getting Started Guide*.

WEBsweeper konfigurieren

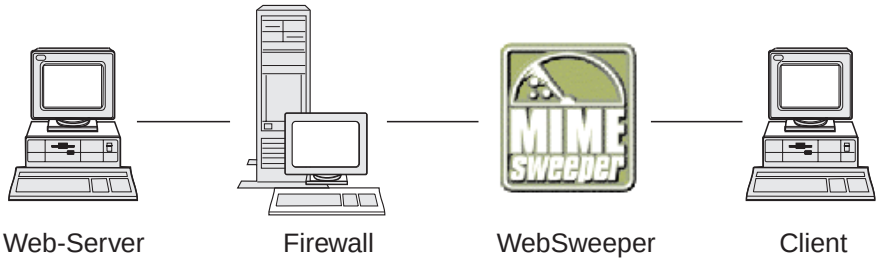

Abbildung 5. WEBsweeper-Konfigurationen

Rufen Sie zum Konfigurieren die Systemsteuerung auf und wählen Sie die WEBsweeper-Minianwendung aus. Weitere Informationen enthält das Buch *WEBsweeper Administrator's Guide*, das sich auf der MIMEsweeper-CD befindet.

WEBsweeper HTTPS konfigurieren

Rufen Sie zum Konfigurieren die Systemsteuerung auf und wählen Sie die WEBsweeper HTTPS-Minianwendung aus. Weitere Informationen enthält das Buch *WEBsweeper Administrator's Guide*.

Abwehren von Eindringlingen

Benutzen Sie die Befehlszeilendienstprogramme, um Filter zu erstellen, mit denen bestimmte IP-Adressen blockiert werden können. Die zu blockierenden Adressen können als Ergebnis der Prüfung des Inhalts dynamisch ermittelt werden.

Es gibt folgende Befehle:

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

Wird das Programm ohne Parameter aufgerufen, erscheint eine Eingabeaufforderung, in der das Format der erforderlichen Parameter eingegeben werden muß.

Es gibt folgende Parameter:

Filter-ID **Für Firewall für Windows NT gilt folgendes:** Filtern kann zwecks Identifikation eine ID zugeordnet werden. Die Zuordnung der IDs erfolgt aufsteigend sortiert und beginnt mit 1. Wird eine ID angegeben, die höher als die nächste verfügbare ID-Nummer ist, wird als ID die als nächste verfügbare ID-Nummer und nicht die angegebene ID zugeordnet. Bestehen beispielsweise Regeln mit der ID-Nummer 1 und versuchen Sie, eine Gruppe von Filterregeln mit der ID-Nummer 3 zu erstellen, wird nicht die ID-Nummer 3, sondern die ID-Nummer 2 zugeordnet. Derselben ID-Nummer können mehrere Regeln zugeordnet werden. Werden Regeln über das Programm fwdelete_dynamic gelöscht, wird als Verweis auf diese Regeln die ID benutzt. Achten Sie beim Erstellen von Regeln anhand von IDs daher darauf, daß sie als Gruppe gelöscht werden können, wenn ihnen dieselbe ID zugeordnet wurde.

Wurde die Regel hinzugefügt, wird die benutzte ID-Nummer angezeigt.

Filter-ID **Für Firewall für AIX gilt folgendes:** Eine ID kann anhand einer Nummer zugeordnet werden. Wollen Sie beispielsweise die Filter-ID 12 angeben, wird sie als ID=12 zugeordnet. Unter AIX ist es nicht möglich, mehreren Filtern dieselbe ID-Nummer zuzuordnen. Jeder Filter hat eine eigene eindeutige ID.

Quellen-IP-Adresse
Die IP-Adresse für die Quelle der Pakete muß in Schreibweise mit Trennzeichen eingegeben werden, beispielsweise 255.255.255.255.

Quellen-IP-Maske
Dieses Feld wird in Verbindung mit der Quellen-IP-Adresse benutzt und in Schreibweise mit Trennzeichen eingegeben. Wurde beispielsweise die Quellen-IP-Adresse 10.5.8.0 eingegeben und ist die Quellen-IP-Maske 255.255.255.0, werden alle Pakete von 10.5.8.1 bis 10.5.8.255 abgeglichen.

Ziel-IP-Adresse
Die IP-Adresse für das Ziel der Pakete muß in Schreibweise mit Trennzeichen eingegeben werden, beispielsweise 255.255.255.255.

Ziel-IP-Maske
Dieses Feld wird in Verbindung mit der Ziel-IP-Adresse benutzt und in Schreibweise mit Trennzeichen eingegeben. Wurde beispielsweise die Ziel-IP-Adresse 10.5.8.0 eingegeben und ist die Ziel-IP-Maske 255.255.255.0, werden alle Pakete von 10.5.8.1 bis 10.5.8.255 abgeglichen.

Adapter Für die Adapterspezifikation gilt folgendes:

- **S** für gesicherte Adapter
- **N** für ungesicherte Adapter
- **B** für alle Adapter (gesicherte und ungesicherte)

Pakete, die von den Adaptern stammen, die mit der angegebenen Adapterart übereinstimmen, entsprechen der Regel.

Bereich Mit diesem Parameter wird der Bereich des Paketdurchlaufs durch die Firewall angegeben. Einer der folgenden Werte ist möglich:

- **L** für lokale Pakete
- **R** für weitergeleitete Pakete
- **B** für lokale und weitergeleitete Pakete

Richtung Gibt an, ob der Datenverkehr ankommt, abgeht oder sowohl ankommt als auch abgeht.

- **I** für ankommenden Datenverkehr
- **O** für abgehenden Datenverkehr
- **B** für ankommenden und abgehenden Datenverkehr

Protokollierung

Geben Sie Y ein, wenn Sie die Protokollierung für das dynamische Filtern einschalten wollen. Geben Sie N ein, wenn Sie die Protokollierung für das dynamische Filtern ausschalten wollen.

fwdelete_dynamic

Wird dieser Befehl ohne Parameter eingegeben, werden alle definierten dynamischen Filter aufgelistet.

```
>>>>  Dynamic Rule Id           =  1
 >>>>>>>>  Jump                 =  0
 >>>>>>>>  Filter Action        =  Deny
 >>>>>>>>  Source Address       =  9.192.8.7
 >>>>>>>>  Source Mask          =  255.255.255.0
 >>>>>>>>  Destination Address  =  9.192.240.1
 >>>>>>>>  Destination Mask     =  255.255.255.0
 >>>>>>>>  Protocol             =  Any
 >>>>>>>>  Source Port          =  Any 0
 >>>>>>>>  Destination Port     =  Any 0
 >>>>>>>>  Adapter              =  Both (Secure and NonSecure)
 >>>>>>>>  Scope                =  Both (Routed and Local)
 >>>>>>>>  Direction            =  Both (Inbound and Outbound)
 >>>>>>>>  Tunnel Id            =  0
 >>>>>>>>  Logging Enabled      =  Unavailable
 >>>>>>>>  Fragments Allowed    =  No
```

Anmerkung: Mit dem Befehl `fwdelete_dynamic` sollte zuerst überprüft werden, ob die zu löschenden Regeln die erwartete ID haben.

Wird der Befehl mit einer gültigen Filter-ID eingegeben, werden die dynamischen Regeln gelöscht, und die Anzahl der gelöschten Regeln wird angezeigt.

ACHTUNG: Wenn Sie versuchen, eine bereits vorhandene Filter-ID hinzuzufügen, erhalten Sie die Mitteilung, daß bereits ein Filter vorhanden ist. Wenn Sie versuchen, einen Filter ohne Angabe einer Filter-ID hinzuzufügen, erscheint eine Warnung.

Das Abwehren von Eindringlingen kann in AIX außer Kraft gesetzt werden, wenn in dem Regelsatz der oberen Ebene Regeln vorhanden sind. Wird das Abwehren von Eindringlingen benutzt, müssen sich die meisten Regeln in dem Regelsatz der unteren Ebene befinden. Dynamische Regeln werden in der Mitte dieser beiden Regelsätze hinzugefügt. Befindet sich eine Regel in der oberen Ebene, die den Datenverkehr zuläßt, können Sie den Datenverkehr nicht über dynamische Regeln verhindern.

Konfiguration testen

Haben Sie alle Konfigurationsaufgaben in den vorhergehenden Kapiteln ausgeführt, muß die Konfiguration getestet werden. Gehen Sie wie folgt vor, um die SecureWay Boundary Server-Konfiguration zu testen:

1. Konfigurieren Sie einen Firewall-Proxy-Benutzer mit dem Policy Director. Legen Sie fest, daß der Benutzer für ein gesichertes Telnet-Protokoll ein Firewall-Kennwort verwenden muß und legen Sie das Kennwort für den Benutzer fest.
2. Richten Sie mit dem SecureWay Boundary Server-Assistenten die Verbindung zwischen der Firewall und dem Directory (LDAP) ein.
3. Starten Sie von einem gesicherten Client eine Proxy-Telnet-Sitzung.
4. Geben Sie die Benutzerkonfiguration über den Policy Director ein.
5. Sie werden zur Eingabe eines Kennworts aufgefordert.
6. Jetzt sind Sie authentifiziert.

Kapitel 6. Referenzliteratur

Die in diesem Kapitel aufgeführten Dokumentationen enthalten weitere Informationen über IBM SecureWay Boundary Server Version 2.0 und zugehörige Produkte.

IBM SecureWay FirstSecure

Das Buch *IBM SecureWay FirstSecure Planung und Integration Version 2.0* enthält Informationen über FirstSecure. In diesem Buch werden FirstSecure und die Produkte beschrieben, die zu FirstSecure gehören. Zudem wird die Planung des Einsatzes der IBM SecureWay-Produkte beschrieben.

IBM SecureWay Firewall

Die folgenden Dokumente enthalten Informationen über IBM SecureWay Firewall für Windows NT und sind in PDF- und HTM-Format im Verzeichnis `x:\books` in verschiedenen Sprachen auf der IBM SecureWay Firewall-CD verfügbar:

- *IBM SecureWay Firewall für Windows NT Konfiguration und Installation*
- *IBM SecureWay Firewall für Windows NT Benutzerhandbuch*
- *IBM SecureWay Firewall für Windows NT Referenzhandbuch*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3* (ein Redbook)

Die folgenden Dokumente enthalten Informationen über IBM SecureWay Firewall für AIX und sind in PDF- und HTM-Format im Verzeichnis `x:\books` in verschiedenen Sprachen auf der IBM SecureWay Firewall-CD verfügbar:

- *IBM SecureWay Firewall für AIX Konfiguration und Installation*
- *IBM SecureWay Firewall für AIX Benutzerhandbuch*
- *IBM SecureWay Firewall für AIX Referenzhandbuch*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (ein Redbook)

MIMEsweeper

MAILsweeper

Die folgenden Dokumente enthalten Informationen über MAILsweeper und sind in PDF- und HTM-Format unter `\install` auf der MIMEsweeper-CD verfügbar:

- *Getting Started Guide* befindet sich in der Datei \install\MSW4_0_2\Doc\qsg.pdf.
- Die Informationsdatei befindet sich in der Datei \install\MSW4_0_2\README.htm

WEBsweeper

Die folgenden Dokumente enthalten Informationen über WEBsweeper und sind in PDF- und HTM-Format unter `\install` auf der MIMEsweeper-CD verfügbar:

- *WEBsweeper Administrator's Guide* befindet sich in der Datei \install\WSW3_2_5\Doc\manual.pdf.
- Die Release-Beschreibung befindet sich in der Datei \install\WSW3_2_5\Doc\RELNOTES.htm.

WEBsweeper HTTPS-Proxy

Das folgende Dokument enthält Informationen über den WEBsweeper HTTPS-Proxy und ist in TXT-Format unter `\install` auf der MIMEsweeper-CD verfügbar:

- Die Informationsdatei befindet sich in der Datei \install\WSWHTTPS1_0_2\readme.txt

SurfinGate

Die folgenden Dokumente enthalten Informationen über SurfinGate und sind in PDF-Format unter `\docs` auf der SurfinGate-CD verfügbar:

- *SurfinGate Installation Guide* befindet sich in der Datei \Docs\install.pdf.
- *SurfinGate User's Manual* befindet sich in der Datei \Docs\manual.pdf.
- Die Release-Beschreibung befindet sich in der Datei \Docs\SFG 405 RelNotes.pdf.
- Informationen über das SurfinGate-Plug-In befinden sich im Verzeichnis `\docs`.

Anhang A. Fehlerbehebung

Dieses Kapitel ist beim Erkennen und Beheben von Problemen hilfreich, die bei dem SecureWay Boundary Server auftreten können.

Allgemeine Probleme mit IBM SecureWay Firewall beheben

Weiterleitungsprobleme

IBM Firewall stellt über die Anzeige **Sicherheitsrichtlinien** die Funktion *IP-Weiterleitung testen* zur Verfügung, die beim Beheben von Weiterleitungsproblemen nützlich sein kann. Aktivieren Sie dieses Kontrollkästchen, aktivieren Sie die Verbindungskonfiguration und aktivieren Sie die Verbindungsregelprotokollierung. Überprüfen Sie dann im `Firewall-Protokoll` die detaillierten Informationen über alle Pakete, die die Firewall durchlaufen haben.

Führen Sie diese Tests zunächst mit IP-Adressen und dann mit Host-Namen aus.

Kein Befehl PING für Hosts aus Firewall möglich

Erklärung des Problems

Die Netzschnittstelle ist nicht korrekt konfiguriert.

Empfohlene Aktion

Siehe Dokumentation des Betriebssystems.

Erklärung des Problems

Die Verbindung zu dem ungesicherten Netz ist nicht korrekt konfiguriert.

Empfohlene Aktion

Nehmen Sie Kontakt zu Ihrem Internet Service Provider auf.

Erklärung des Problems

Wenn das gesicherte Netz hinter einem Router isoliert ist, benötigt die Firewall einen statischen Leitweg zu diesem Router. Überprüfen Sie die statische Weiterleitung mit dem Befehl `netstat -rn`:

```
netstat -rn
```

Die Ausgabe muß für die Protokollfamilie 2 wie folgt aussehen:

```
Destination  Gateway          Flags     ....
default      nrr.nrr.nrr.nrr  UG
nnn.nnn.nnn  nnn.nnn.nnn.nnn  U
sss.sss.sss  sss.sss.sss.sss  U
ss1.ss1.ss1  srr.srr.srr.srr  UG
127          127.0.0.1        U
```

Abbildung 6. Beispielausgabedaten des Befehls netstat -rn.

nrr.nrr.nrr.nrr
steht für den Router zum Internet und ist der Standardleitweg. Der Standardleitweg ist ein statischer Leitweg (Flag=UG).

nnn.nnn.nnn
steht für die ungesicherte Domäne. Dies ist ein Schnittstellenleitweg (Flag=U).

nnn.nnn.nnn.nnn
steht für die ungesicherte Schnittstelle.

sss.sss.sss
steht für die gesicherte Domäne. Dies ist ein Schnittstellenleitweg (Flag=U).

sss.sss.sss.sss
steht für die gesicherte Schnittstelle.

ss1.ss1.ss1
steht für eine Unterdomäne auf der gesicherten Seite des Netzes, und srr.srr.srr.srr steht für den Router zu dieser Unterdomäne. Dieser Leitweg ist ein statischer Leitweg (Flag=UG).

127.0.0.1
ist die Loopback-Adresse oder der lokale Host. Dies ist ein Schnittstellenleitweg (Flag=U).

Für jede Schnittstelle muß ein Schnittstellenleitweg vorhanden sein, und der Standardleitweg muß auf den Router auf der ungesicherten Seite der Firewall zeigen.

Empfohlene Aktion
Fügen Sie dem Router einen statischen Leitweg hinzu. Nehmen Sie Kontakt mit dem Router-Administrator auf. Benutzen Sie den Befehl `route add`.

Erklärung des Problems
Möglicherweise ist die Teilnetzmaske auf der gesicherten Schnittstelle oder der Host, mit dem Kontakt aufgenommen werden sollte, falsch.

Empfohlene Aktion
Korrigieren Sie die Maskeneinstellungen über die Client-Konfigurationsdienstprogramme.

Kein Befehl PING für ungesicherte Hosts aus gesicherten Hosts (oder umgekehrt) möglich

Erklärung des Problems

Jeder der Firewall benachbarte Router muß einen statischen Leitweg enthalten, in dem die Firewall als Gateway für Zielnetze hinter der Firewall angegeben ist.

Empfohlene Aktion

Nehmen Sie Kontakt mit dem Router-Administrator auf.

Erklärung des Problems

Wenn das gesicherte Netz Adressen benutzt, die nicht registriert sind und auf dem ungesicherten Netz nicht weitergeleitet werden können (auch private Adressen, siehe RFC 1597), werden Pakete nicht an den Absender zurückgeleitet.

Empfohlene Aktion

Nur für Windows NT: Benutzen Sie einen Client mit einer registrierten Adresse. Für den TCP- und UDP-Datenverkehr kann die Funktion für Netzadressenumsetzung der Firewall benutzt werden, aber die Netzadressenumsetzung setzt keine Adressen in ICMP-Paketen um. ICMP-Pakete werden beispielsweise gesendet, wenn der Befehl PING abgesetzt wird.

Empfohlene Aktion

Nur für AIX: Benutzen Sie einen Client mit einer registrierten Adresse.

DNS-Fehler

Anmerkung: DNS bezieht sich nur auf Windows NT.

Erklärung des Problems

Es wurden DNS-Fehlernachrichten gesendet, da Microsoft DNS mit dem Microsoft DNS-Manager konfiguriert wurde.

Empfohlene Aktion

Gehen Sie anhand der Installationsanweisungen vor und

1. entfernen Sie Microsoft DNS durch Löschen des Verzeichnisses `\winnt\system32\DNS`.
2. Installieren Sie Microsoft DNS erneut.
3. Starten Sie das System neu.
4. Installieren Sie den DNS-Hotfix erneut.
5. Starten Sie das System neu.

Allgemeine Probleme mit MIMEsweeper beheben

WEBsweeper und MAILsweeper scheinen auf derselben Maschine nicht zu funktionieren

Erklärung des Problems

Es treten Probleme auf, wenn MAILsweeper und WEBsweeper auf derselben Maschine ausgeführt werden sollen.

Empfohlene Aktion

Installieren Sie MAILsweeper und WEBsweeper auf separaten Maschinen.

Geringe Leistung von WEBsweeper

Erklärung des Problems

Das Herunterladen von Web-Inhalt dauert bei der Benutzung von WEBsweeper zu lange.

Empfohlene Aktion

1. Inaktivieren Sie die Protokollierung über die WEBsweeper-Minianwendung, die über die Systemsteuerung aufgerufen werden kann.
2. Installieren Sie WEBsweeper auf der schnellsten Hardware, die verfügbar ist.

Probleme mit der WEBsweeper-Lizenzierung

Erklärung des Problems

Wird WEBsweeper 3.2_5 auf einer Maschine installiert, auf der bereits eine frühere WEBsweeper-Version installiert war, kann ein Lizenzberechtigungskonflikt auftreten. Wird WEBsweeper gestartet und erscheint eine Nachricht über einen internen Windows-Fehler (2140), überprüfen Sie das Anwendungsprotokoll in der Ereignisanzeige. Die Nachricht von WEBsweeper lautet: "PAKMSG error: Username conflicts with previously defined license section."

Empfohlene Aktion

Entfernen Sie die alte Lizenzberechtigung aus der Windows-Registrierung. Geben Sie den Befehl `regedit` ein und suchen Sie unter dem Pfad \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License nach Lizenzberechtigungen. Befinden sich dort mehrere Lizenzberechtigungen, löschen Sie die Lizenzberechtigung, die nicht mit "IBM MIMEsweeper System" gekennzeichnet ist. Starten Sie das System neu.

WEBsweeper hat Probleme beim Herunterladen großer Dateien

Erklärung des Problems

Möglicherweise reicht der virtuelle Speicher von WEBsweeper nicht aus, um Dateien beim Filtern zu speichern.

Empfohlene Aktion

Erhöhen Sie den physischen Speicher auf dem WEBsweeper-Server.

Allgemeine Probleme mit SurfinGate beheben

SurfinConsole antwortet bei geöffnetem Microsoft Internet Explorer nicht mehr

Erklärung des Problems

Die Anwendung SurfinConsole verhält sich bei geöffnetem Microsoft Internet Explorer nicht wie erwartet oder antwortet bei geöffnetem Microsoft Internet Explorer nicht mehr. Zwischen diesen beiden Anwendungen besteht ein Konflikt, und sie können nicht gleichzeitig ausgeführt werden.

Empfohlene Aktion

Laden Sie den Internet Explorer und die SurfinConsole nicht gleichzeitig.

Geringe Leistung des SurfinGate-Plug-Ins

Erklärung des Problems

Das Herunterladen von mobilem Code über das Web dauert bei Benutzung des SurfinGate-Plug-Ins sehr lange.

Empfohlene Aktion

Achten Sie darauf, daß das Feld **Next Proxy** im Abschnitt **Proxy** der SurfinConsole auf den SecureWay Firewall-HTTP-Proxy gesetzt ist.

Anhang B. Bemerkungen

Hinweise auf IBM Produkte, Programme und Dienstleistungen in dieser Veröffentlichung bedeuten nicht, daß IBM diese in allen Ländern, in denen IBM vertreten ist, anbietet. 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 oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

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.

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):

Site Counsel, IBM SWG
IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

Dieses Programm wird nicht unter den Allgemeinen Geschäftsbedingungen der IBM, sondern unter den "Internationalen Nutzungsbedingungen der IBM für Programmpakete" lizenziert.

Die Veröffentlichung dient nicht für Produktionszwecke. IBM übernimmt keine Haftung. Die in dieser Veröffentlichung aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.

Dieses Produkt enthält Computersoftware, die von CERN erstellt oder zur Verfügung gestellt wurde. Ein entsprechender Hinweis ist in allen Produkten enthalten, die CERN-Computersoftware oder Komponenten dieser Software enthalten.

Marken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

AIX

IBM

Microsoft und Windows NT sind Marken der Microsoft Corporation.

SurfinGate ist eine Marke der Finjan Software, Ltd.

MIMEsweeper, MAILsweeper und WEBsweeper sind Marken der Content Technologies, Ltd.

Mit ** gekennzeichnete Namen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Glossar

A

Anschluß. Eine Nummer, mit der die Kurzform einer DFV-Einheit identifiziert wird. Web-Server benutzen standardmäßig den Anschluß 80.

Assistent. Ein Dialog innerhalb einer Anwendung, der Benutzer Schritt für Schritt durch eine bestimmte Aufgabe führt.

C

Client. Ein Datenverarbeitungssystem oder ein Prozeß, das/der einen Service eines anderen Datenverarbeitungssystems oder Prozesses anfordert, das/der normalerweise als Server bezeichnet wird. Mehrere Clients können gemeinsam auf einen allgemeinen Server zugreifen.

D

DMZ. Demilitarized Zone. Eine Einheit, die verhindert, daß externe Benutzer direkt auf einen Server mit Unternehmensdaten zugreifen können.

F

Firewall. Eine Funktionseinheit, die die Verbindung eines Netzes zu anderen Netzen schützt und steuert. Die Firewall verhindert unerwünschte oder unbefugte Datenübertragungen in das gesicherte Netz und ermöglicht nur ausgewählten Datenübertragungen das Verlassen des gesicherten Netzes.

FTP (File Transfer Protocol). Ein Anwendungsprotokoll, das benutzt wird, um Dateien in und aus vernetzten Computern zu übertragen. Für FTP ist eine Benutzer-ID und manchmal auch ein Kennwort erforderlich, um auf Dateien auf einem fernen Host-System zugreifen zu können.

G

Gateway. Eine Funktionseinheit, die zwei Computernetze mit unterschiedlichen Architekturen miteinander verbindet.

I

ICMP. Internet Control Message Protocol. Das Protokoll wird zur Behandlung von Fehlern und zur Steuerung von Nachrichten in der IP-Schicht (Internet Protocol Layer) benutzt. Fehlerberichte und falsche Datagrammzieladressen werden an die ursprüngliche Datagrammquellenadresse zurückgegeben.

Internet. Die weltweite Gruppe miteinander verbundener Netze, die die Internet-Protokollgruppe verwenden und allgemein zugänglich sind.

Intranet. Ein gesichertes privates Netz, das Internet-Standards und -Anwendungen (beispielsweise Web-Browser) in die vorhandene Computernetzinfrastruktur eines Unternehmens integriert.

IP. Internet Protocol. Ein Protokoll für virtuelle Verbindungen, das Daten in einem Netz oder in miteinander verbundenen Netzen weiterleitet. Das Internet Protocol agiert als Vermittler zwischen den höheren Protokollschichten und der Bitübertragungsschicht.

IP-Adresse. Internet Protocol-Adresse. Die eindeutige 32-Bit-Adresse, mit der die aktuelle Position der einzelnen Einheiten oder Workstations in einem Netz angegeben wird. Die Internet Protocol-Adresse wird auch als Internet-Adresse bezeichnet.

IPSEC. Internet Protocol Security (Internet Protocol-Sicherheit). Ein aufkommender Standard für die Sicherheit in der Vermittlungs- oder Paketverarbeitungsschicht der Netzkommunikation.

L

Loopback-Schnittstelle. Eine Schnittstelle, die unnötige Übertragungsfunktionen umgeht, wenn die Informationen an eine Definitionseinheit innerhalb desselben Systems adressiert werden.

N

NAT. Network Address Translation (Netzadressenumsetzung). In einer Firewall die Umsetzung von gesicherten IP-Adressen in extern registrierte Adressen. Auf diese Weise ist die Kommunikation mit externen Netzen möglich, aber die innerhalb der Firewall benutzten IP-Adressen werden maskiert.

P

PICS. Platform for Internet Content Selection. Durch PICS-fähige Clients können die Benutzer festlegen, welche Leistungsservices sie benutzen wollen und welche Leistungsstufen der einzelnen Leistungsservices akzeptabel und nicht akzeptabel sind.

Ping. Ein Befehl, der ICMP-Echoanforderungspakete an einen Host, Gateway oder Router sendet und eine Antwort erwartet.

Protokoll. Eine Reihe von Regeln, die den Betrieb von Funktionseinheiten eines DFV-Systems steuern, wenn eine Übertragung erfolgen soll. Über Protokolle ist es möglich, Details der niedrigen Ebene für Schnittstellen zwischen Maschinen (beispielsweise die Reihenfolge, in der die Bit eines Byte gesendet werden) oder den Austausch auf hoher Ebene zwischen Anwendungsprogrammen (beispielsweise Dateiübertragung) festzulegen.

S

Server. Ein Computer, der gemeinsame Services für andere Computer über ein Netz liefert, beispielsweise ein Datei-Server, ein Druck-Server oder ein Post-Server.

Server-Adresse. Der eindeutige Code, der einem Computer zugeordnet wird, der gemeinsame Services für andere Computer über ein Netz liefert, beispielsweise ein Datei-Server, ein Druck-Server oder ein Post-Server. Eine Standard-IP-Adresse ist ein 32-Bit-Adreßfeld. Die Server-Adresse kann als IP-Adresse in Schreibweise mit Trennzeichen oder als Host-Name angegeben werden.

Service. Eine Funktion, die von Knoten zur Verfügung gestellt wird (beispielsweise HTTP, FTP, Telnet).

Shell. Die Software, die Befehlszeilen einer Workstation des Benutzers akzeptiert und verarbeitet. Die Korn-Shell ist beispielsweise eine von mehreren verfügbaren UNIX-Shells.

SMTP. Simple Mail Transfer Protocol. In der Internet-Protokollgruppe ein Anwendungsprotokoll zur Übertragung von Post zwischen Benutzern in der Internet-Umgebung. SMTP gibt die Reihenfolge des Postaustauschs und das Nachrichtenformat an. SMTP nimmt TCP (Transmission Control Protocol) als untergelegtes Protokoll an.

Standardwert. Ein Wert, ein Attribut oder ein Parameter, der/das angenommen wird, wenn kein Wert, Attribut oder Parameter explizit angegeben wird.

T

TCP. Transmission Control Protocol. Ein Übertragungsprotokoll, das im Internet benutzt wird. TCP ermöglicht den zuverlässigen Austausch von Informationen zwischen Hosts. TCP benutzt IP (Internet Protocol) als untergelegtes Protokoll.

TCP/IP. Transmission Control Protocol/Internet Protocol. Eine Protokollgruppe, die eine von den Übertragungstechnologien in den einzelnen Netzen unabhängige Übertragung zwischen Netzen ermöglicht.

Telnet. Terminal-Emulationsprotokoll, ein TCP/IP-Anwendungsprotokoll für Fernverbindungsservice. Telnet bietet dem Benutzer die Möglichkeit, so auf einen fernen Host zuzugreifen, als ob die Workstation des Benutzers direkt mit diesem fernen Host verbunden wäre.

U

UDP. User Datagram Protocol. In der Internet-Protokollgruppe ein Datagrammprotokoll für virtuelle Verbindungen. Es ermöglicht einem Anwendungsprogramm auf einer Maschine oder einem Prozeß das Senden eines Datagramms an ein Anwendungsprogramm auf einer anderen Maschine oder einem anderen Prozeß. UDP benutzt das Internet Protocol (IP) zur Zustellung von Datagrammen.

V

VPN. Virtuelles Privates Netz. Ein Netz, das aus gesicherten IP-Tunneln besteht, über die Netze miteinander verbunden werden.

W

Web. Das Netz von HTTP-Servern, die Programme und Dateien enthalten, von denen viele Hypertext-Dokumente mit Verbindungen zu anderen Dokumenten auf HTTP-Servern sind. Wird auch World Wide Web genannt.

WTE. Web Traffic Express. Ein Caching-Proxy-Server, der die Antwortzeiten für Endbenutzer durch leistungsfähige Caching-Schemata verbessern kann. Durch flexible PICS-Filterung können Netzadministratoren den Zugriff auf web-gestützte Informationen von einem zentralen Standort aus steuern.

Z

Zeitlimit. Ein für eine bestimmte Operation vorgesehenes Zeitintervall.

Antwort

IBM SecureWay Boundary Server
für Windows NT und AIX
Installation und Konfiguration
Version 2.0

IBM Teilenummer CT6RZDE

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: CT6RZDE

Printed in Denmark

CT6RZDE