Windows NT® 및 AIX용 IBM SecureWay®
Boundary Server

시작에서 수행까지

버전 2.0

GA30-1012-00

Windows NT® 및 AIX용 IBM SecureWay®
Boundary Server

시작에서 수행까지

버전 2.0

GA30-1012-00

주

이 책과 이 책에서 지원하는 제품을 사용하기 전에 47 페이지의 『부록B. 주의사항』에 있는 일반 정보를 읽으십시오.

이 책은 개정판에 특별한 언급이 없는 한 IBM SecureWay Boundary Server 제품(GA30-1012-00)의 버전 2, 릴리스 0, 수정판 0 및 모든 후속 릴리스와 수정판에 적용됩니다.

재판(1999년 10월)

목차

이 책에 대하여

이 책은 Windows NT® 및 AIX용 IBM SecureWay®Boundary Server 계획, 설치, 구성, 사용 그리고 문제 해결 방법에 대해 설명합니다.

이 책의 사용자는 SecureWay Boundary Server를 설치하고 구성하기 전에 Firewall, VPN, Content Security 및 네트워크 관리에 대해 상당한 지식을 가지고 있는 것이 중요합니다. 네트워크 내외에서 이루어지는 액세스를 제어하는 Firewall을 설정하고 구성하므로 먼저 네트워크 작동 방법에 대해 이해해야 합니다. 특히, IP 주소, 완전한 이름 그리고 서브네트 마스크의 기본을 이해해야 합니다.

이 책의 사용자

이 책은 네트워크나 IBM SecureWay Boundary Server를 설치, 관리 그리고 사용하는 시스템 보안 관리자를 위한 것입니다.

2000년 대비

이들 제품은 2000년에 대한 준비가 되어 있습니다. 관련 문서에 따라 사용되는 경우 이는 20 세기와 21 세기 간에 날짜 데이터를 올바로 처리, 제공 그리고 수신할 수 있습니다. 단, 이 제품과 함께 사용되는 모든 제품(예를 들어, 하드웨어, 소프트웨어 그리고 펌웨어)이 정확한 날짜 데이터를 제대로 교환할 수 있어야 합니다.

서비스 및 지원

IBM SecureWay FirstSecure 제품에 포함된 모든 제품의 서비스와 지원에 대해서는 IBM에 문의하십시오. 이런 제품 중 일부는 IBM 이외의 지원을 요구할 수도 있습니다. 이런 제품을 FirstSecure 제품의 일부로 받는 경우 IBM에 문의하여 서비스와 지원을 받으십시오.

이 책의 구성

이 책은 다음과 같은 장으로 구성됩니다.

- 1 페이지의 『제1장 SecureWay Boundary Server 개요』는 SecureWay Boundary Server와 그 구성요소의 개요를 제공합니다.
- 5 페이지의 『제2장 IBM SecureWay Boundary Server 소개』는 SecureWay Boundary Server가 필요한 이유에 대한 정보를 제공합니다.
- 21 페이지의 『제5장 SecureWay Boundary Server 설치 및 구성』은 Windows NT 및 AIX 운영 체제에서의 SecureWay Boundary Server의 설치와 구성을 설명합니다.
- 13 페이지의 『제3장 SecureWay Boundary Server를 설치하기 전에』은 SecureWay Boundary Server의 계획 방법에 대한 정보를 제공합니다.
- 19 페이지의 『제4장 IBM SecureWay Boundary Server(SBS) 요구사항』은 SecureWay Boundary Server의 최소 요구사항에 대한 정보를 제공합니다.
- 39 페이지의 『제6장 관련 문서』는 SecureWay Boundary Server의 기타 문서와 관련 제품의 문서를 찾을 수 있는 위치를 알려줍니다.

용례

이 책에서는 다음과 같은 규칙을 사용합니다.

용례	의미
굵은체	선택란, 단추 그리고 명령과 같은 사용자 인터페이스 요소
모노스페이스	SecureWay Boundary Server에 관련된 구문과 디렉토리 기본값
->	메뉴에서 일련의 선택항목을 보여줍니다. 예를 들어, **파일**-> **실행**을 선택하면 **파일**을 누른 후 **실행**을 누르라는 것과 같습니다.

웹 정보

SecureWay Boundary Server에 대한 최신 갱신 정보는 다음 웹 주소에서 얻을 수 있습니다.

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

기타 IBM SecureWay FirstSecure 제품에 대한 정보는 다음 웹 주소에서 얻을 수 있습니다.

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

새로운 기능

SecureWay Boundary Server의 버전 2.0에는 몇 가지 새로운 기능이 들어 있습니다. 가장 중요한 새 기능은 다음과 같습니다.

SecureWay Policy Director와의 통합

SecureWay Policy Director는 Firewall이 SecureWay Boundary Server를 사용할 수 있는 경우 Firewall 프록시 사용자를 관리할 수 있습니다. Firewall 프록시 사용자는 다음 Firewall 서비스에 대해 정의됩니다.

- 텔넷
- FTP
- HTTP
- Socks

사용자와 그 관련된 정책은 LDAP(Lightweight Directory Access Protocol) 데이터베이스에 저장됩니다.

SecureWay Directory는 저장, 갱신, 검색 및 교환에 대해 중앙 위치에서 디렉토리 정보를 유지보수할 수 있도록 LDAP를 제공합니다. SecureWay Policy Director는 LDAP 데이터베이스에서 Firewall 프록시 사용자를 관리합니다.

라우팅 효율성

라우팅 효율성은 내용 필터링에서 네트워크 트래픽의 회로를 단축하기 위해 Finjan SurfinGate 플러그인을 사용합니다.

침입 차단

명령 행은 Firewall에서 동적 DENY 규칙을 작성하기 위해 프로그램합니다. 침입 차단은 자동 스크립트에 통합될 수 있습니다.

IBM SecureWay Firewall 4.1

Windows NT용 IBM SecureWay Firewall은 다음을 제공합니다.

원격 액세스 서비스

Windows NT 원격 액세스 서비스(RAS)는 다이얼 업, ISDN 또는 PPP(Point-to-Point Protocol)를 사용하는 X.25 미디어를 통해 네트워크 연결을 제공합니다. NDISWAN은 RAS의 일부로 제공되고 이더넷 LAN 데이터와 유사하도록 기초를 이루는 PPP 데이터를 변환하는 네트워킹 드라이버입니다.

AIX 4.1용 IBM SecureWay Firewall 향상

AIX용 IBM SecureWay Firewall은 다음을 제공합니다.

향상된 IPSec 지원

IBM SecureWay Firewall 4.1에는 3중-DES 암호화, 새 헤더의 지원을 포함하는 향상된 IPSec 지원이 있습니다. 이는 또한 여러 IBM 서버 및 라우터와의 상호 조작 가능성뿐만 아니라 새 헤더를 지원하는 많은 비-IBM VPN 제품을 지원합니다.

대칭 다중프로세서(SMP)

Firewall 사용자는 확장과 성능 향상을 위해 RS/6000의 다중프로세서 기능을 사용할 수 있습니다.

필터 향상

필터는 구성에서 더 나은 성능을 제공할 수 있도록 향상되었습니다. 필터 규칙의 다른 유형을 찾을 위치를 선택하여 Firewall의 성능을 조정할 수 있습니다. 이 외에도, 연결을 사용하는 횟수가 기록됩니다.

설정 마법사

마법사는 IBM SecureWay Firewall의 초기 구성을 지원합니다. 이 설정 마법사는 새 사용자가 IBM Firewall 설치 이후에 기본 Firewall 구성을 시작하고 신속하게 실행할 수 있게 합니다.

네트워크 보안 감사기

네트워크 보안 감사기(NSA)는 네트워크 서버와 Firewall에서 보안 틈이나 구성 오류를 점검합니다. 이는 더 빠르고 더 견고하게 향상되었습니다.

독일어에 대한 자국어 지원

독일어에 대한 자국어 지원은 이제 브라질어, 포르투갈어, 영어, 프랑스어, 이탈리아어, 일본어, 한국어, 대만어, 스페인어 그리고 중국어 외에 추가로 제공됩니다.

네트워크 주소 변환

네트워크 주소 변환(NAT)은 다-대-일 주소 맵핑을 지원할 수 있도록 향상되었습니다. 이런 맵핑은 여러 미등록 주소 또는 사설 주소에서 포트 번호를 사용하여 고유한 맵핑을 작성하는 등록된 적법한 주소로 이루어집니다.

AIX 및 Windows NT에서 지원하는 공통 기능

Security Dynamics ACE/Server

Security Dynamics ACE/Server는 인증의 두 가지 요인을 제공합니다. 이 기능은 향상되고 잠재적인 사고나 고의에 의한 침입으로부터 네트워크와 데이터 자원을 보호합니다.

보안 메일 프록시 향상

IBM Firewall 보안 메일 프록시는 다음과 같은 새 기능을 포함하여 더욱 향상되었습니다.

- 알려진 SPAMers(제외 목록)의 메시지 차단, 메시지 유효성과 응답 가능성에 대한 검증 확인(원하지 않는 메시지를 차단하는 알려진 방법),

메일 메시지별 수신인 수에 대해 구성 가능한 한계, 최대 메시지 크기에 대한 구성 가능한 한계 등을 포함하는 반-SPAM 알고리즘

- 강력한 인증 메커니즘과의 통합을 포함하는 anti-spoofing 지원
- SNMP 트랩 지원 및 MADMAN MIB에 대한 지원
- Firewall과 Domino 간에 메시지를 연속으로 추적할 수 있는 기능을 포함한 메시지 추적

Socks 프로토콜 버전 5 향상

Socks 프로토콜 버전 5는 사용자 ID-암호 인증(UNPW), 도전/응답 인증(CRAM) 그리고 인증 플러그인을 포함하기 위해 업그레이드되었습니다.

기록은 사용자에게 로그 메시지를 분류하고 기록 레벨을 지정할 때 더 많은 제어권을 제공하기 위해 향상되었습니다.

HTTP 프록시

IBM SecureWay Firewall은 IBM WTE(Web Traffic Express) 제품을 기반으로 한 완전하게 갖춘 HTTP 프록시 구현을 제공합니다. HTTP 프록시는 IBM Firewall을 통해 브라우저 요청을 효율적으로 처리하므로 웹 찾아보기에서 socks 서버가 필요없게 됩니다. 사용자는 내부 네트워크의 보안을 손상시키지 않고 인터넷에서 유용한 정보를 액세스할 수 있습니다. 브라우저는 HTTP 프록시를 사용할 수 있도록 구성되어야 합니다.

SecureWay용 MIMEsweeper 2.0

MIMEsweeper에는 **MAILsweeper 4.1_2**, **WEBsweeper 3.2_5** 그리고 **WEBsweeper 1.0_2**의 3 가지 주요 구성요소가 있습니다. 일부 향상은 다음과 같습니다.

MAILsweeper

SMTP용 MAILsweeper 4.1_2는 Content Technologies의 최신 MIMEsweeper 제품으로의 주요 업그레이드입니다. 이는 다음과 같은 새 기능을 제공합니다.

- 사용하기 쉬운 계층적 정책 구조는 적합한 조직적 레벨에서 개별 사용자까지 모두 정책을 적용할 수 있는 융통성을 제공합니다.
- 산업 표준 그래픽 사용자 인터페이스(GUI)는 소프트웨어 구성, 정책 작성 및 관리 작업을 단순화합니다.

- 새 분할 전달 기능은 버전 4의 계층적 정책 구현의 기능입니다. 수신인이 여러 명인 메시지에 대해 정책은 각 수신인에게 적용됩니다. 권한을 부여 받은 수신인은 메시지를 받는 반면 권한을 부여 받지 못한 수신인은 거부됩니다.
- 다중 스레드 메시지 처리는 처리량을 향상시키고 오류가 하나 이상의 스레드에서 발생할 때 나머지 스레드를 통해 메시지 처리를 계속 진행할 수 있도록 하여 견고함을 추가할 수 있습니다.
- 기타 공급업체의 바이러스 방지 제품과 연계하여 MAILsweeper는 바이러스 발견 및 메시지와 첨부 정리 기능을 제공합니다.
- NEAR, AND, NOT 그리고 OR 표현을 사용하는 고급 텍스트 분석은 메시지 구문이나 구조를 기반으로 한 포괄적이고 효과적인 시나리오 작성에 있어서 엄청난 융통성을 제공합니다.
- ODBC 호환 가능 데이터베이스에 데이터를 전송하는 향상된 감사 툴.
- 불필요한 이메일을 전송하는 것으로 알려진 사이트를 나열하는 RBL(Real-Time Black List) 서버를 지원합니다. MAILsweeper는 이 목록에 있는 호스트와의 연결을 거부할 수 있습니다.
- Content Security는 이메일 트래픽의 매력적인 보고서/그래프/차트를 통해 관리하는 것이 더 쉽습니다.
- LDAP 디렉토리와의 통합
- DSN(Delivery Service Notification)은 이제 SNMP와 NT 경보기를 지원합니다.

WEBsweeper

- 추가 성능 향상은 데이터 처리 속도를 향상시킵니다.
- HTTP와 FTP 트래픽에 대한 바이러스 스캐너와 함께 작업합니다.

WEBsweeper HTTPS

- WEBsweeper는 이제 새 HTTPS 프록시 솔루션을 통해 웹 기반의 전자 상거래 응용 프로그램에 대한 완전한 지원을 제공합니다.

SurfinGate 4.05

SurfinGate 향상에는 다음이 포함됩니다.

JavaScript 내용 검사

SurfinGate 4.05는 잠재적으로 문제를 일으킬 수 있는 JavaScript 작업을 찾아보고 회사 보안 정책과 충돌하는 JavaScript를 중지합니다. SurfinGate 4.05를 통해 관리자는 VisualBasic 스크립트와 쿠키에 대한 스마트 필터링과 함께 JavaScript, Java 그리고 ActiveX에 대한 정책을 중앙에서 설정하고 강제 적용합니다.

임무 중요 성능 모니터링

SurfinGate 4.05에는 비정상적인 동작(예를 들어, 런타임 오류)을 발견하고 장애의 경우 SurfinGate를 다시 시작하는 자동 툴이 들어 있습니다. 이는 임무 중요 영역에서 중요한 보안 기능입니다.

증가된 정책 관리

SurfinGate는 자동 차단을 위해 분석되지 않은 애플릿 프로파일을 데이터베이스에 입력합니다. 관리자는 애플릿/제어 목록을 편집할 수 있습니다.

FTP 및 SSL 프로토콜 지원

SurfinGate 4.05는 모빌 코드에 대해 FTP(File Transfer Protocol) 채널을 모니터하면서 모르는 사이에 인터넷에 끼어 들어갈 수 있는 코드를 감시합니다. FTP 외에 SurfinGate는 모빌 코드에 대해 HTTP 트래픽을 모니터하고 HTTPS 트래픽을 추가 장치로 전달합니다.

Firewall HTTP 프록시와의 플러그인 통합

SurfinGate는 프록시 체인에서 프록시로 작동하거나 Windows NT용 Firewall의 WTE에 있는 플러그인을 통해 프록시로 작동합니다.

제1장 SecureWay Boundary Server 개요

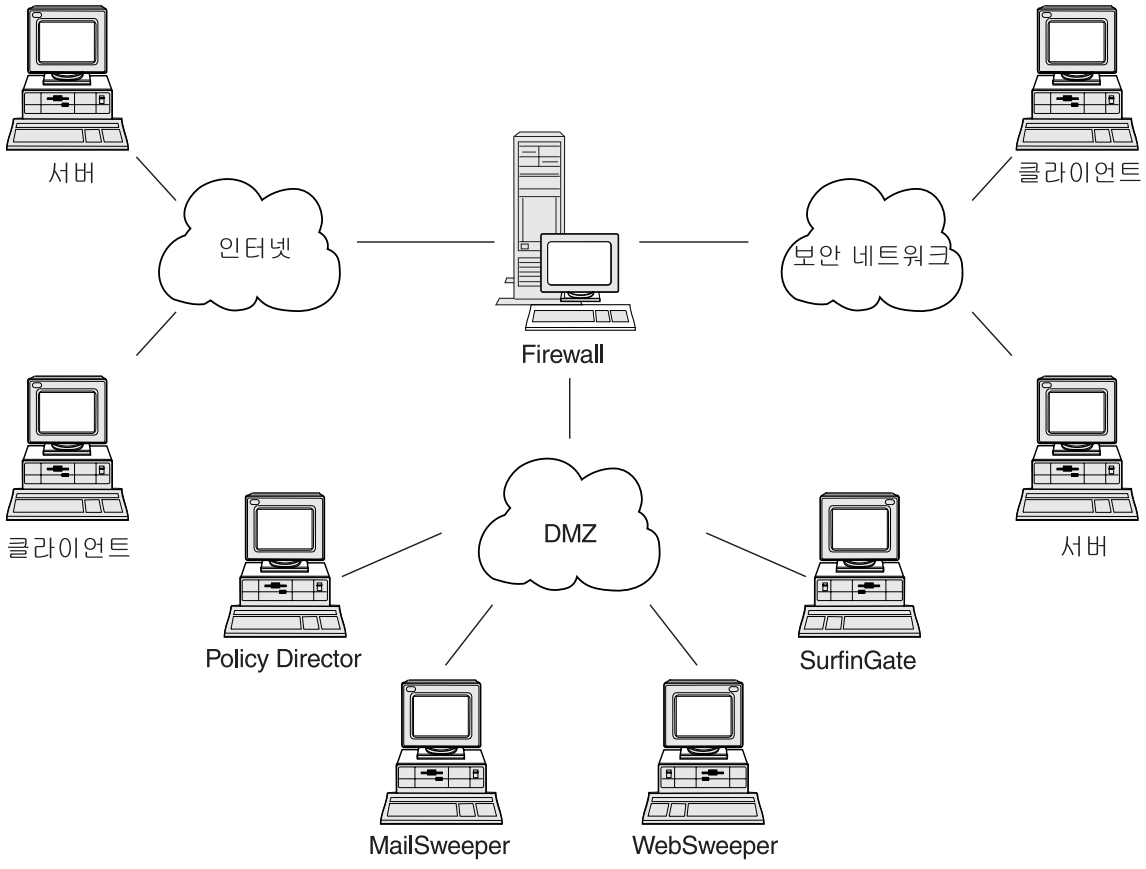

그림 1. IBM SecureWay Boundary Server 구성 예제

이 예제는 MAILsweeper, WEBsweeper, Policy Director 그리고 SurfinGate 구성요소를 사용하여 Firewall을 사용하는 클라이언트와 서버 간에 웹 트래픽과 메일을 모니터하고 경로 지정하는 5개의 워크스테이션을 보여줍니다. 이 예제에서 실제로 분리된 5개의 워크스테이션을 사용합니다.

일반적인 SecureWay Boundary Server 예제

최소 설정을 위해 다음과 같은 시스템을 사용하는 것이 바람직합니다.

표 1. Boundary Server 구성요소 제품을 위한 하드웨어 요구사항

제품	시스템
IBM Firewall	Windows NT 또는 AIX
MAILsweeper	Windows NT
WEBsweeper	Windows NT
SurfinGate	Windows NT

SecureWay Boundary Server를 충분히 활용하려면 네트워크에 SecureWay Policy Director가 있어야 합니다. 이를 통해 Firewall 프록시 사용자를 SecureWay Directory(LDAP)에 저장할 수 있습니다.

HTTP 예제(Windows NT Firewall): 일반적인 시나리오에서 인터넷 내용에 대한 HTTP 요청은 클라이언트 시스템에서 시작합니다. 요청은 먼저 WEBsweeper로 이동합니다. 아웃바운드 경로에서 요청은 WEBsweeper에 의해 Firewall HTTP 프록시로 프록시됩니다.

Firewall HTTP 프록시에서 사용자는 인증됩니다. 이것이 클라이언트 세션의 첫 요청이면 사용자 ID/암호를 입력해야 합니다. 사용자 ID는 Policy Director에서 관리하는 LDAP 데이터베이스에 있는 클라이언트의 보안 정책을 찾는데 사용됩니다. 클라이언트에 대한 HTTP 인증 정책과 입력된 암호 확인 결과에 따라 요청을 거부하거나 계속 진행하도록 허용할 수 있습니다. 인증 작업에서는 LDAP 데이터베이스나 Security Dynamics ACE 서버를 더 액세스해야 되는 경우도 있습니다. 같은 세션의 후속 요청에 대해 브라우저는 사용자 ID/암호를 자동으로 제공합니다. 클라이언트에서 사용자 ID/암호를 요구하지 않지만 첫 요청과 같은 프로세스를 통해 각 요청은 계속 인증됩니다.

제대로 인증된 경우 요청은 인터넷에서 요청된 서버로 프록시됩니다.

Firewall HTTP 프록시에서 인터넷 서버의 내용을 다시 수신하면 SurfinGate 플러그인에서 이를 조사합니다. LDAP 데이터베이스에서 얻은 사용자의 그룹 정보는 정책 결정의 기준으로 삼을 수 있도록 플러그인에서 사용할 수 있게 됩니다. 내용에 SurfinGate에게 중요한 내용이 없으면 이는 최소한의 처리 오버헤드와 함께 플러그인을 빠르게 통과합니다. JavaScript가 들어 있는 내용은 플러그인에서 필

터됩니다. Java나 ActiveX가 들어 있는 내용은 SurfinGate 서버로 전달되어 필터되고 필터된 내용은 Firewall HTTP 프록시로 리턴됩니다. SurfinGate 플러그인 처리 결과인 내용은 다시 WEBsweeper 서버로 전송됩니다.

내용이 다시 WEBsweeper 서버로 돌아오면 WEBsweeper 정책에 따라 필터되고 클라이언트로 다시 리턴됩니다.

HTTP 예제(AIX Firewall): AIX에서 트래픽의 흐름은 AIX Firewall에서 사용할 수 있는 SurfinGate 플러그인이 없는 경우를 제외하고는 본질적으로 동일합니다. 그러므로, SurfinGate 서버는 클라이언트에서 Firewall까지 이루어진 프록시 체인에서 프록시로 설정되어야 합니다. WEBsweeper는 요청을 직접 Firewall HTTP 프록시로 전달하는 대신 SurfinGate 서버로 전달하도록 설정되어야 합니다. 그러면 SurfinGate 서버는 요청을 Firewall HTTP 프록시로 전달하도록 구성해야 합니다. SurfinGate 서버에서 그룹 정보를 사용할 수 없으므로 정책 결정은 IP 주소만을 기준으로 삼습니다.

메일 예제: MAILsweeper는 메일 게이트웨이로 설정됩니다. MAILsweeper 서버에 도착하는 메일은 다음 메일 서버로 전달되기 전에 그 내용이 필터됩니다.

보안 메일 서버마다 클라이언트 메일 요청을 MAILsweeper 서버로 전달하도록 구성해야 합니다. Firewall 메일 교환기를 구성하여 수신 메일을 MAILsweeper 서버로 전달해야 합니다.

MAILsweeper는 주소가 외부 도메인으로 되어 있는 메일을 Firewall 메일 교환기로 전송할 수 있도록 구성되어야 합니다. MAILsweeper는 주소가 내부 도메인으로 되어 있는 메일을 올바른 보안 메일 서버로 전송할 수 있도록 구성되어야 합니다.

제2장 IBM SecureWay Boundary Server 소개

본 장에서는 SecureWay Boundary Server 개요를 제공하며 다음과 같은 섹션으로 이루어져 있습니다.

- 『SecureWay Boundary Server 정의』
- 6 페이지의 『SecureWay Boundary Server가 필요한 이유』
- 6 페이지의 『FirstSecure에 SecureWay Boundary Server를 맞추는 방법』
- 6 페이지의 『SecureWay Boundary Server의 구성요소』

SecureWay Boundary Server 정의

IBM SecureWay Boundary Server는 처음으로 완벽한 경계 보안 솔루션을 한자리에 모아 놓았습니다. SecureWay Boundary Server는 Firewall 보호, VPN(virtual private network) 그리고 Content Security를 제공합니다. SecureWay Boundary Server는 보안 산업의 기술을 IBM의 지원과 서비스로 뒷받침되는 통합된 솔루션에 모아 놓았습니다. 이 솔루션에는 다음이 들어 있습니다.

- IBM SecureWay Firewall 4.1(Security Dynamic ACE/Server 포함)
- Content Technologies의 MIMEsweeper
  - MAILsweeper 4.1_2
  - WEBsweeper 3.2_5
  - WEBsweeper HTTPS 프록시 1.0_2
- Finjan의 SurfinGate 4.05
  - SurfinGate 서버
  - SurfinConsole
  - SurfinGate 데이터베이스
  - Windows NT 1.0용 WTE 통합에 대한 SurfinGate 플러그인

SecureWay Boundary Server가 필요한 이유

보안 경계는 엔지니어링 및 인적 자원과 같은 부서 간, 본사 네트워크와 지사 간, 사내 네트워크와 인터넷 간, 회사의 웹 응용 프로그램과 고객 간, 사내 네트워크나 응용 프로그램과 영업 파트너 간 등 모든 곳에 필요합니다. 경계 보안은 네트워크, 응용 프로그램 및 정보를 보호할 뿐만 아니라 그 범위를 확장하기도 합니다. 적절한 경계 보안에서는 네트워크를 액세스할 수 있는 자와 네트워크에서 입력되거나 출력되는 정보를 제어할 수 있습니다.

FirstSecure에 SecureWay Boundary Server를 맞추는 방법

IBM SecureWay FirstSecure는 통합된 제품의 패키지입니다. 이는 인터넷과 기타 네트워크에서 이루어지는 네트워킹의 모든 측면을 보안할 수 있도록 포괄적인 프레임워크를 제공합니다. 이는 현재 투자한 것 위에 상호 작용 가능한 모듈의 방식으로 구축하고 보안 e-business 소유권의 총 비용을 최소화하는데 도움을 줍니다. 이는 바이러스로부터 보호해 주고 액세스 제어, 트래픽 내용 제어, 암호화, 디지털 인증, Firewall, 툴킷 그리고 구현 서비스를 제공합니다.

Boundary Server는 FirstSecure에 맞는 제품 패키지입니다. 이는 잠재적으로 유해한 바이러스(보조 바이러스 스캔 제품 사용), JavaScript, Java 애플릿, ActiveX 제어 그리고 필요없는 이메일(SPAM)을 차단할 때 사용할 수 있는 인터넷에 대한 경계를 만듭니다. Boundary Server를 가지고 인터넷에서 네트워크로 입력할 내용을 정확하게 제어할 수 있습니다. SecureWay Policy Director를 사용하면 Firewall 프록시 사용자와 그 인증 정책을 관리할 수 있습니다.

SecureWay Boundary Server의 구성요소

SecureWay Boundary Server의 3가지 구성요소는 IBM Firewall, MIMEsweeper 및 SurfinGate입니다. SecureWay Boundary Server는 IBM SecureWay Policy Director와 통합됩니다.

IBM SecureWay Boundary Server 개요

IBM SecureWay Boundary Server는 큰 규모의 조직이 그 엔터프라이즈를 고객, 공급업자 그리고 파트너에게 안전하게 개방하여 전자 상거래에 있어서 필요한 보호, 액세스 제어 그리고 Content Security를 제공합니다. 기능에는 다음이 포함됩니다.

- 네트워크에 대한 Firewall 보호
- 네트워크의 범위를 확장하기 위한 VPN(Virtual Private Network)
- 회사의 데이터, 이미지 그리고 신뢰도와 생산성을 보호하기 위한 이메일 및 웹 트래픽에 대한 내용 스캐너

SecureWay Boundary Server는 그 분야에서 최고의 기술을 IBM의 지원과 서비스로 뒷받침되는 통합된 솔루션에 모아 놓았습니다. 이는 AIX와 Windows NT 운영 체제에서 사용 가능합니다.

SecureWay Boundary Server 기능

SecureWay Boundary Server는 패킷 필터링, 프록시 및 Socks 서버 기술과 Content Security를 적용하여 네트워크와 시스템을 숨기고 보호합니다. 이런 기술을 통해 관리자는 네트워크와 주고 받을 수 있는 데이터를 명시적으로 정의할 수 있습니다. 이는 "서비스 공격의 거부"와 해커가 네트워크에 침입하여 적법한 의무를 제한하지 못하도록 방지하는데 도움을 줍니다. SecureWay Boundary Server는 VPN 솔루션을 제공하여 원격 서버와 모뎀 뱅크를 인터넷 기반 솔루션으로 대체할 수 있게 합니다.

Policy Director, SecureWay Boundary Server는 중앙 정책 기반 계획을 사용하여 사용자 인증을 제공합니다. SecureWay Boundary Server에서 바이러스 방지 소프트웨어를 사용하여 사용자 사이트를 바이러스로부터 보호할 수 있습니다.

IBM SecureWay Policy Director 개요

Policy Director는 지리적으로 분산되어 있는 인트라넷과 엑스트라넷에서 자원을 완벽하게 보안하는 독립형 권한 부여 및 보안 관리 솔루션입니다. 엑스트라넷은 액세스 제어와 보안 기능을 사용하여 선택된 가입자가 인터넷에 접속된 하나 이상의 인트라넷을 사용하는 경우 그 범위를 제한하는 VPN(virtual private network)입니다. Policy Director는 인증, 권한 부여, 데이터 보안 그리고 자원 관리 서비스

를 제공합니다. Policy Director를 표준 인터넷 기반 응용 프로그램과 연계하여 안전하고 잘 관리된 인트라넷과 엑스트라넷을 구축할 수 있습니다.

IBM SecureWay Policy Director 기능

SecureWay Boundary Server와 함께 사용하는 경우 IBM SecureWay Policy Director는 프록시 사용자 정책과 인증 정보의 저장영역을 제공합니다.

IBM SecureWay Firewall 개요

IBM SecureWay Firewall은 네트워크 보안 프로그램입니다. Firewall은 하나 이상의 사설 내부 보안 네트워크와 기타 네트워크나 인터넷 간의 차단막입니다. Firewall은 원하지 않거나 권한이 부여되지 않은 통신이 보안 네트워크에 들어가거나 나오지 않도록 막아줍니다.

IBM SecureWay Firewall 기능

IBM SecureWay Firewall은 보호된 네트워크, 인터넷 그리고 기타 네트워크 세트 간에 이루어지는 액세스를 제한합니다. 이는 또한 다음을 수행합니다.

- 신중히 제어된 포인트에 사람들이 들어가지 못하도록 제한합니다.
- 공격자가 기타 방어막에 접근하지 못하도록 막습니다.
- 사람들이 신중히 제어된 포인트에서 나오지 못하도록 제한합니다.
- 내부 Firewall은 권한이 부여되지 않은 직원이 중요한 내부 정보에 접근하지 못하도록 분리합니다.
- 네트워크에 들어가거나 나올 수 있는 트래픽을 제한합니다.

MIMEsweeper 개요

MIMEsweeper는 전자 우편이나 월드 와이드 웹을 통해 Firewall을 통과하는 데이터를 분석하여 Content Security를 제공합니다. Content Security를 통해 조직은 이메일과 월드 와이드 웹 사용에 관련된 업무 문제를 효과적으로 관리할 수 있습니다. 이런 문제는 네트워크 통합성과 업무 통합성으로 나눌 수 있습니다.

네트워크 통합성 필터링으로 다음을 수행할 수 있습니다.

- 수신 또는 송신 이메일에 있는 바이러스를 식별하고 제거합니다.
- 원하지 않는 파일 유형을 필터합니다.

- 너무 큰 파일을 관리합니다.
- 정체나 메일 훼손 공격으로 인한 서비스 유실로부터 네트워크를 보호합니다.

업무 통합성 필터링으로 다음을 수행할 수 있습니다.

- 기밀 누설과 거래 기밀의 유실을 막습니다.
- 적법한 의무의 노출을 제한합니다.
- 직원이 이메일과 월드 와이드 웹 서비스를 잘못 사용하여 유실되는 양을 줄입니다.
- 잘못 사용하거나 적대적인 공격으로 인한 네트워크 서비스 유실로부터 보호합니다.

네트워크 통합성을 위협하면 데이터는 훼손되거나 지워지고 이메일 흐름은 중단되며 시스템 하드웨어가 훼손될 수 있으므로, 이 모든 것에 의해 네트워크가 중단되고 생산성이 저하되며 비싼 정리 및 복구 비용이 들게 됩니다.

그러나 업무 통합성을 위협하면 훨씬 더 파괴적이어서 엄청난 법적 비용이 들게 되고 지적 등록정보가 유실되며 회사의 명성과 신뢰도에 타격을 입게 됩니다. 업무 통합성 문제는 업무를 정지시킬 수 있습니다.

MIMEsweeper는 조직에서 이메일과 인터넷을 사용하여 발생하는 네트워크 및 업무 통합성 문제로부터 조직을 보호하는 업계를 선도하는 제품입니다.

MIMEsweeper 기능

MIMEsweeper는 다음을 수행할 수 있습니다.

- 적법한 거부자를 아웃바운드 메일에 추가합니다.
- 기밀 문서와 데이터를 보호합니다.
- 이메일과 웹 기반 사용자에게 권한을 부여하고 제어합니다.
- 적대적인 자료를 격리하거나 차단합니다.
- 불필요한 이메일을 차단합니다.
- 첨부를 스캔하고 적합한 내용을 다운로드합니다.
- 바이러스와 유해한 코드를 중지합니다.
- 부적절한 웹 페이지와 사이트를 차단합니다.

- 보고, 로그 및 보존합니다.

SurfinGate 개요

SurfinGate 4.05는 업무 트랜잭션에 인터넷, 엑스트라넷 또는 인트라넷을 사용하는 모든 업무의 모빌 코드 보안 툴입니다. JavaScript를 포함한 모빌 코드의 내용 검사를 통해 SurfinGate는 적대적이거나 산업 첩보 활동, 데이터 수정 그리고 정보 삭제를 포함한 부지 불식간의 훼손으로부터 컴퓨터 네트워크를 보호할 수 있도록 지원합니다. SurfinGate의 내용 검사 프로세스는 중요한 자원에서 떨어져 있는 게이트웨이 레벨에서 Java, JavaScript 그리고 ActiveX 모빌 코드 내용을 검사하고 가능한 보안 누수를 알리는 코드에 고유한 ID와 애플릿 보안 프로파일(ASP)을 할당합니다. SurfinGate는 잠재적으로 문제를 일으킬 수 있는 코드가 네트워크에 들어 가기 전에 이를 식별합니다.

SurfinGate 4.05에는 4가지 구성요소가 있습니다.

- SurfinGate 서버
- SurfinConsole
- SurfinGate 데이터베이스
- Windows NT용 WTE 통합에 대한 SurfinGate 플러그인

SurfinGate 서버는 HTTP 프록시 서버로 작동합니다. SurfinGate는 Firewall HTTP 프록시와 WEBsweeper 프록시와 함께 프록시 체인의 일부로 배치할 수 있습니다. Windows NT에 대해 이를 Firewall HTTP 플러그인에 대한 플러그인으로 사용될 수도 있습니다. 플러그인으로 사용되는 경우 SurfinGate는 요청하는 프록시 사용자에 대해 그룹 정보를 가져옵니다. SurfinGate 필터링 정책은 이 그룹 정보를 기준으로 합니다. 이 구조에서는 시스템 공격이 발생하기 전에 모빌 코드 트래픽을 정지하고 검토할 수 있습니다. 이 구성요소는 회사 보안 정책별로 보호를 제공합니다.

SurfinConsole은 모빌 코드에 대해 중앙 회사 보안 정책을 관리하고 설정하는 사용자에게 친숙한 인터페이스입니다. SurfinConsole은 네트워크에서 여러 SurfinGate 서버를 제어할 수 있고 사용자나 그룹별 회사 전반에 걸쳐 또는 사용자 설치 목록이나 허용 불능 및 허용 가능 코드를 통해 모빌 코드 규칙을 강제 실행할 수 있습니다.

SurfinGate 데이터베이스는 사용자와 그룹 그리고 그 해당 보안 정책에 관한 정보를 포함하여 애플릿 보안 프로파일(ASP)의 세부사항을 저장합니다. 데이터베이스는 내장된 액세스 데이터베이스 엔진이나 기존의 Oracle 데이터베이스를 사용할 수 있습니다. SurfinGate는 모든 모빌 코드의 내용을 동적으로 조사하므로 데이터베이스는 보안에 필요 없지만 대규모의 조작에서 성능 향상에 도움을 줍니다.

SurfinGate의 기능

SurfinGate는 다음을 제공합니다.

- Java 애플릿, ActiveX 제어, JavaScript에 대한 게이트웨이 레벨 내용 조사 서버
- 실시간 모니터링, 동적 조사
- 웹 기반 모빌 코드에 대한 보안 정책 강제 실행
- ″모빌 코드″(예를 들어, Java 애플릿, ActiveX 제어, JavaScript, Visual Basic 스크립트, 플러그인, 쿠키)의 조사

SurfinGate는 프록시 체인에서 또는 Windows NT용 Firewall의 WTE 플러그인을 통해 프록시와 함께 작동할 수 있습니다.

제3장 SecureWay Boundary Server를 설치하기 전에

본 장에서는 마법사를 사용하여 SecureWay Boundary Server 설치를 준비하는 방법을 보여줍니다. 이는 다음과 같은 섹션으로 이루어져 있습니다.

- 『준비 방법』
- 16 페이지의『SecureWay Boundary Server』

준비 방법

본 섹션에서는 SecureWay Boundary Server의 구성요소를 준비하는 방법을 보여줍니다.

SecureWay Policy Director와의 통합

Windows NT나 AIX에서 기본 IBM SecureWay Policy Director를 설정하려면 다음을 수행하십시오.

1. 운영 체제가 Policy Director를 지원할 수 있도록 제대로 구성되어 있는지 확인합니다.
2. 전개 요구사항에 가장 잘 맞는 서버 구성요소와 이런 구성요소를 설치할 시스템을 결정합니다.
3. DCE 하부구조가 없는 경우에는 이를 설치하고 구성합니다.
4. SecureWay Directory(LDAP)를 설치하고 구성합니다.
5. 클라이언트 인증서를 인증하는 경우에는 CAS(Certificate Authorization Service)를 구성합니다.
6. NetSEAT 클라이언트를 설치합니다.
7. Policy Director 서버 구성요소를 설치합니다.
8. 관리 콘솔을 설치합니다.

Policy Director에 대한 자세한 내용은 *Policy Director Up and Running 3.0*을 참조하십시오.

SecureWay Firewall

Windows NT나 AIX에서 기본 IBM Firewall을 설정하려면 다음을 수행하십시오.

1. 19 페이지의 『SecureWay Boundary Server의 하드웨어 요구사항』에 나열된 요구사항을 갖추고 있는지 확인합니다.
2. IBM Firewall 설정을 계획합니다. 미리 사용할 Firewall 기능과 그 용도를 결정합니다.
3. Firewall에게 네트워크 보안을 위해 그 인터페이스 중 어떤 것이 연결되어 있는지 알려줍니다. Firewall이 제대로 작동하려면 보안 인터페이스와 비보안 인터페이스가 있어야 합니다. 구성 클라이언트 탐색 트리에서 시스템 관리 폴더를 열고 **인터페이스**를 눌러 Firewall에 있는 네트워크 인터페이스 목록을 봅니다. 인터페이스의 보안 상태를 변경하려면 인터페이스를 선택하고 **변경**을 누릅니다.

   주: 인터넷에 접속하려면 ISP(Internet Service Provider)에 연결하여 Firewall 비보안 인터페이스의 등록된 IP 주소를 확보합니다.
4. 시스템 관리 폴더에서 **보안 정책** 대화 상자를 액세스하여 일반 보안 정책을 설정합니다. 일반적인, Firewall 구성에 대해
   - DNS 조회를 허용합니다
   - 비보안 인터페이스에 대한 브로드캐스트 메시지를 거부합니다
   - 비보안 어댑터에 대한 Socks를 거부합니다
5. 도메인 이름 서비스와 메일 서비스를 설정합니다. DNS 해상도를 제공하지 않으면 효율적인 통신이 이루어지지 않습니다. 구성 클라이언트 탐색 트리의 시스템 관리 폴더에서 이런 기능을 액세스합니다.
6. 구성 클라이언트 탐색 트리의 **네트워크 오브젝트** 기능을 사용하여 Firewall에서의 네트워크(들) 주요 요소를 정의합니다. 네트워크 오브젝트는 Firewall을 통해 트래픽을 조절합니다. 다음 주요 요소를 네트워크 오브젝트로 정의하십시오.
   - Firewall의 보안 인터페이스
   - Firewall의 비보안 인터페이스
   - 보안 네트워크
   - 보안 네트워크에서의 각 서브네트

- 해당하는 경우 Security Dynamics 서버와 Windows NT 도메인 서버에 대한 호스트 네트워크 오브젝트

7. Firewall에서 서비스를 사용할 수 있게 합니다. 이는 보안 네트워크에 있는 사용자가 비보안 네트워크를 액세스할 때 사용하는 메소드(예를 들어, socks 또는 프록시)입니다. 구현되는 서비스는 계획 단계에서 이루어지는 결정에 의해 달라집니다. 서비스를 구현할 때 특정 유형의 트래픽을 허용하려면 일부 연결 구성을 설정해야 합니다. 예를 들어, 보안 사용자가 HTTP 프록시를 사용하여 인터넷의 웹을 탐색할 수 있게 하려면 Firewall의 HTTP 프록시 디먼을 구성할 뿐만 아니라 연결을 설정하여 HTTP 트래픽을 허용해야 합니다. Policy Director를 설정하는 경우 13 페이지의 『SecureWay Policy Director와의 통합』를 참조하십시오.
8. **Windows NT 전용:** 더욱 어려워지는 프로세스에 의해 NETBIOS를 사용할 수 없게 되므로 인증에서 Windows NT 도메인 암호를 사용하려면 인증하기 위해 신뢰할 수 있는 Windows NT 도메인을 탐색할 수 있는 기능을 구현하는 Windows 클라이언트 코드를 구성해야 합니다. 신뢰할 수 있는 Windows NT 서버에는 TCP/IP 호스트 이름과 주소가 있어야 하며 이와 Firewall 사이에는 TCP/IP 연결성이 있어야 합니다. Firewall 관리자는 Firewall과 신뢰할 수 있는 Windows NT 서버를 연결하여 서로 간에 트래픽이 흐르도록 해야 합니다.
9. 네트워크 주소 변환을 사용하는 경우 먼저 ISP에 접속하여 다-대-일 주소 변환에 사용할 등록된 인터넷 주소를 확보하십시오. 이 주소는 14 페이지의 3 단계에서 요청한 주소에 추가한 것입니다. 그런 후 *NAT 구성 추가* 패널로 이동하여 등록된 인터넷 주소를 *다-대-일 IP 주소* 필드에 추가하십시오.

이런 단계를 수행하면 기본 Firewall 구성이 실행됩니다. IBM Firewall은 네트워크 보안을 확인할 수 있도록 시스템 로그와 같은 기타 기능을 제공합니다.

Firewall이 정상적으로나 비정상적으로 종료하는 경우 구성 데이터는 하드 드라이브에 저장되고 다시 부팅할 때 자동으로 다시 활성화되므로 영향을 받지 않습니다. 그러나, 활성화된 FTP 세션과 같은 일부 활성화된 연결이 인터럽트되었음을 알려주는 특정 Firewall 로그 메시지가 발생합니다.

SecureWay Boundary Server

SecureWay Boundary Server 마법사를 사용하여 Policy Director와 통합하기 위해 사용자 관리에서 IBM SecureWay Policy Director를 사용할 수 있도록 Firewall을 설정합니다. 선택적으로, 이 마법사는 Firewall HTTP 프록시를 구성하여 인증 정보를 SurfinGate 플러그인(Windows NT 전용)에 전달합니다.

Firewall에 대해 IBM SecureWay Boundary Server를 구성할 때 필요한 정보는 다음과 같습니다.

- Firewall이 사용할 IBM SecureWay Directory 서버의 호스트 이름과 도메인.
- IBM SecureWay Directory 서버가 청취하는 포트의 수. 기본 포트는 389입니다.
- IBM SecureWay Directory 서버의 SecurityMaster 암호.
- 이 Firewall에서 프록시 사용자를 구분하기 위해 사용하는 도메인 이름. 이 이름을 사용하는 모든 Firewall은 같은 사용자 세트를 관리합니다. 일반적으로, Firewall 시스템의 완전한 호스트 이름을 사용하게 됩니다.
- SecureWay Directory에 저장된 프록시 사용자를 액세스할 때 사용하는 Firewall 관리자 이름. 이 이름은 SecureWay Policy Director에서 작성된 모든 프록시 사용자를 수정할 수 있도록 액세스가 허용됩니다. Firewall 시스템의 완전한 호스트 이름을 사용해야 합니다.
- IBM SecureWay Directory가 데이터베이스에서 Firewall 사용자 탐색을 시작하는 루트로 사용하는 DN(Distinguished Name). 이는 Policy Director 사용자를 저장하기 위해 SecureWay Directory에서 작성한 접미사이어야 합니다.
- IBM SecureWay Directory 서버에 연결할 때 사용할 Firewall의 관리자 ID의 암호.

Firewall과 SecureWay Directory 서버 사이에 트래픽이 흐르도록 연결을 작성해야 합니다.

19 페이지의 『SecureWay Boundary Server의 하드웨어 요구사항』에 나열된 요구사항을 갖추고 있는지 확인합니다.

SurfinGate

SurfinGate를 사용하려면 Windows NT Service Pack 5가 설치되어 있어야 합니다. 19 페이지의 『SecureWay Boundary Server의 하드웨어 요구사항』에 나열된 요구사항을 갖추고 있는지 확인합니다.

다음을 수행하여 SurfinGate를 사용하십시오.

- Oracle 데이터베이스를 사용하는 경우 이를 구성해야 합니다.
- Windows NT Firewall을 사용하는 경우 플러그인을 사용할 것인지 아니면 프록시 모드를 사용할 것인지 결정해야 합니다.
- WTE에서 SurfinGate 플러그인을 사용하려면 Firewall 시스템에 SurfinGate 플러그인을 설치하고 SecureWay Boundary Server 마법사를 설치합니다.
- SurfinGate 플러그인에서 SurfinGate 서버로 트래픽이 흐르도록 하려면 연결을 작성해야 합니다.

MIMEsweeper

MIMEsweeper를 사용하려면 네트워크의 작동 방법을 이해해야 합니다. 19 페이지의 『SecureWay Boundary Server의 하드웨어 요구사항』에 나열된 요구사항을 갖추고 있는지 확인합니다.

MAILsweeper

: MIMEsweeper를 구성하는 경우 MAILsweeper와 WEBsweeper를 서로 다른 시
: 스템에 설치해야 합니다.

MAILsweeper를 구성하기 전에 다음 작업을 수행하십시오.

- 내부적으로 사용하는 메일 도메인을 결정합니다. MAILsweeper와 Firewall 메일 교환기는 각각의 메일 도메인에 대해 메일을 받을 수 있도록 구성되어야 합니다.
- 도메인을 지원하는 보안 메일 서버를 결정합니다. MAILsweeper는 주소가 메일 도메인으로 되어 있는 메일을 올바른 보안 메일 서버로 전송할 수 있도록 구성되어야 합니다.

- MAILsweeper 서버의 주소를 결정합니다. 각각의 보안 메일 서버는 내부 클라이언트에서 수신한 메일을 MAILsweeper 서버로 전달할 수 있도록 구성되어야 합니다.
- Firewall의 주소를 결정합니다. MAILsweeper는 주소가 외부 도메인으로 되어 있는 메일을 Firewall 메일 교환기로 전달하도록 구성되어야 합니다.

WEBsweeper

WEBsweeper를 구성하기 전에 다음 작업을 수행하십시오.

- WEBsweeper 서버의 주소를 결정합니다. 이는 네트워크의 각 클라이언트 웹 브라우저에서 필요합니다. 브라우저는 WEBsweeper 서버를 HTTP, FTP 그리고 HTTPS의 프록시로 사용할 수 있도록 구성되어야 합니다.
- Firewall의 보안 인터페이스 주소를 결정합니다. WEBsweeper는 프록시 요청을 Firewall에 상주하는 HTTP 프록시로 전달할 수 있도록 구성되어야 합니다.
- 클라이언트가 웹 내용 필터링을 생략하지 않도록 하려면 Firewall에서 연결을 설정하여 WEBsweeper 및/또는 SurfinGate 서버에 대한 프록시 액세스를 제한해야 합니다.

제4장 IBM SecureWay Boundary Server(SBS) 요구사항

본 장에서는 SecureWay Boundary Server의 최소한의 요구사항을 제공합니다.

SecureWay Boundary Server의 하드웨어 요구사항

Boundary Server 구성요소 제품에 대한 하드웨어 요구사항은 다음 표에 있습니다.

표 2. Boundary Server 구성요소 제품을 위한 하드웨어 요구사항

Boundary Server 구성요소	**기계 유형**	**디스크 공간**	**메모리**	**기타**
Policy Director	N/A	64 MB	16 MB	N/A
IBM Firewall	• Windows NT: 266 MHz 이상 • AIX: 4.3.2를 지원하는 RS/6000 시스템	Windows NT: 200 MB AIX: 200 MB	Windows NT: 64 MB AIX: 128 MB	네트워크 인터페이스 카드(NIC) 2개
ACE/Server	• Windows NT: 166 MHz 이상(단일 프로세서만) • AIX: AIX 4.2를 지원하는 기계	• 기본 서버 소프트웨어: 50 MB • 백업 서버: 22MB • 초기 사용자 데이터베이스: 4MB • 설치: 240MB	최소: 32MB	실제 기억장치 필요량은 사용자 수에 따라 다릅니다.
MAILsweeper	Windows NT: 400 MHz 이상의 프로세서	1 GB	128 MB	N/A
WEBsweeper	Windows NT: 450 MHz 이상의 프로세서	1 GB	128 MB	N/A
고볼륨 환경에 대한 WEBsweeper 시스템 요구사항	Windows NT: 450 MHz 이상의 프로세서	3 GB	512 MB	N/A
SurfinGate 4.05 Server	Windows NT: 233 MHz 이상의 프로세서	20 MB	256 MB	N/A

표 2. Boundary Server 구성요소 제품을 위한 하드웨어 요구사항 (계속)

SurfinGate 4.05 Console	Windows NT: 233 MHz 이상의 프로세서	15 MB	64 MB	N/A

주: 자세한 내용에 대해서는 AIX용 IBM SecureWay Firewall이나 여러 언어에 대한 Windows NT 버전 설정 및 설치를 참조하십시오. 또한, Netscape Browser에 대해서는 디스크 공간이 138 MB 필요합니다.

SecureWay Boundary Server에 대한 소프트웨어 요구사항

Boundary Server 구성요소 제품에 대한 소프트웨어 요구사항은 다음 표에 있습니다.

표 3. Boundary Server 구성요소 제품에 대한 최소한의 소프트웨어 요구사항

제품	**Windows**	**AIX**	기타
Policy Director 서버	Service Pack 5가 설치된 Windows NT 버전 4.0	4.3.1	N/A
IBM Firewall	Service Pack 5가 설치된 Windows NT 버전 4.0	4.3.2	N/A
SecureWay Boundary Server	IBM SecureWay Firewall 4.1	IBM SecureWay Firewall 4.1	N/A
MAILsweeper	Service Pack 5가 설치된 Windows NT 버전 4.0, Internet Explorer 4.01 이상, Microsoft Management Console 1.1, NTFS 드라이브, Windows Messaging	N/A	사용할 바이러스 방지 툴
WEBsweeper	Service Pack 5가 설치된 Windows NT 버전 4.0	N/A	사용할 바이러스 방지 툴
SurfinGate Server	Service Pack 5가 설치된 Windows NT 4.0 버전	N/A	N/A
SurfinGate 4.05 Console	Service Pack 5가 설치된 Windows NT 버전 4.0 또는 Windows 95	N/A	N/A

제5장 SecureWay Boundary Server 설치 및 구성

본 장에서는 Windows NT와 AIX에서 SecureWay Boundary Server를 구성하고 설치하는 방법을 알려줍니다.

- 『SecureWay Boundary Server 구성요소 설치』
- 24 페이지의 『SecureWay Boundary Server 구성요소 구성』
- 34 페이지의 『침입 차단』

SecureWay Boundary Server 구성요소 설치

본 섹션에서는 Windows NT와 AIX용 IBM SecureWay Firewall, SurfinGate 그리고 MIMEsweeper를 설치할 수 있도록 도와줍니다.

SecureWay Firewall 설치

Windows NT 및 AIX용 IBM SecureWay Firewall에 대한 자세한 내용은 13 페이지의 『준비 방법』을 참조하십시오. 이는 보안 인터페이스를 정의하는 방법, 보안 정책을 결정하는 방법 그리고 네트워크 오브젝트를 정의하는 방법을 설명합니다. SecureWay Firewall 설치에 대한 자세한 내용은 *IBM SecureWay Firewall Installation Guide for AIX* 및 *IBM SecureWay Firewall Installation Guide for Windows NT*를 참조하십시오.

SecureWay Directory 설치

SecureWay Boundary Server의 LDAP 기능을 사용하는 경우 SecureWay Directory를 설치해야 하는데 *IBM SecureWay Policy Director Up and Running 3.0*을 참조하십시오.

SecureWay Directory 서버는 사용자의 Firewall 보안 내부에 위치해 있거나 Firewall 보안 DMZ에 있습니다.

SecureWay Policy Director 설치

SecureWay Boundary Server의 LDAP 기능을 사용하는 경우 SecureWay Policy Director를 설치해야 합니다(*IBM SecureWay Policy Director Up and Running 3.0* 참조).

SecureWay Boundary Server 설치

Windows NT에서 SecureWay Boundary Server를 설치하려면 다음을 수행하십시오.

- Windows NT용 SecureWay Firewall을 설치합니다.
- SecureWay Boundary Server CD에서 setup.exe를 실행합니다.
- 언어를 선택하고 **확인**을 누릅니다.
- InstallShield는 SecureWay Boundary Server를 어디에 설치하고 싶은지 묻습니다. Windows NT 기본 디렉토리는 C:\Program Files\IBM\SBS입니다.
- 다시 부트합니다.

AIX에서 SecureWay Boundary Server를 설치하려면 다음을 수행하십시오.

- AIX용 SecureWay Firewall을 설치합니다.
- CD를 삽입하고 SMITTY를 사용하여 설치합니다.
- 소프트웨어 설치 및 유지보수를 선택합니다.
- 소프트웨어 설치 및 갱신을 선택합니다.
- 사용 가능한 최신 소프트웨어에서 설치 및 갱신을 선택합니다.
- 입력 장치를 요구하는 경우 선택항목을 나열하고 CD-ROM 드라이브를 선택합니다.
- 설치할 소프트웨어 선택항목을 나열하고 sbs를 선택합니다.
- **Enter**를 눌러 소프트웨어를 설치합니다.
- 다시 부트합니다.

SurfinGate 설치

SurfinGate에는 SurfinGate Server와 SurfinGate Console의 두 구성요소가 있습니다. SurfinGate의 두 구성요소중 하나를 설치하려면 SurfinGate CD의 \docs\install.pdf에 있는 설치 안내서를 참조하십시오.

SurfinGate 플러그인

Windows NT용 IBM SecureWay Firewall에 SurfinGate 플러그인을 설치하려면 SurfinGate CD의 \docs 디렉토리에 위치한 설치 안내서를 참조하십시오.

MIMEsweeper 설치

MIMEsweeper에는 MAILsweeper, WEBsweeper 그리고 WEBsweeper HTTPS 등 3가지 구성요소가 있습니다.

: MAILsweeper 4.1은 NTFS 파티션에 설치되어야 합니다.

MAILsweeper 설치

MAILsweeper를 설치하려면 MIMEsweeper CD의 \install\MSW4_0_2\docs\qsg.pdf에 있는 *Getting Started Guide*를 참조하십시오.

MAILsweeper를 WEBsweeper HTTP 프록시와 같은 시스템에 설치하지 **마십시오.**

MAILsweeper를 WEBsweeper HTTPS 프록시와 같은 시스템에 설치하지 **마십시오.**

WIndows NT CD에서 MAPI32.dll을 설치한 후 MIMEsweeper CD에서 Microsoft 관리 콘솔 1.1을 설치하면 MAPI32.dll의 올바른 버전이 Microsoft 관리 콘솔과 함께 설치된 역 레벨 버전으로 겹쳐쓰여집니다. Microsoft 관리 콘솔을 설치한 후 반드시 MAPI32.dll 버전 4.0 이상을 설치하십시오. dll은 보통 Windows Messaging 구성요소에 있습니다.

WEBsweeper 설치

WEBsweeper를 설치하려면 MIMEsweeper CD의 \install\WSW3_2_5\docs\manual.pdf에 위치한 *관리자 안내서*를 참조하십시오.

: WEBsweeper를 MAILsweeper와 같은 시스템에 설치하지 **마십시오.**

WEBsweeper HTTPS 설치

WEBsweeper HTTPS를 설치하려면 MIMEsweeper CD의 \install \WSWHTTPS1_0_2\readme.txt에 위치한 *Readme*를 참조하십시오.

WEBsweeper HTTPS 프록시를 MAILsweeper와 같은 시스템에 설치하지 **마십시오**.

SecureWay Boundary Server 구성요소 구성

SecureWay Firewall 구성

기본 IBM Forewall 설정에 대해:

1. IBM Firewall 설정을 계획합니다. 미리 사용할 Firewall 기능과 그 용도를 결정합니다.
2. Firewall에게 네트워크 보안을 위해 그 인터페이스 중 어떤 것이 연결되어 있는지 알려줍니다. Firewall이 제대로 작동하려면 보안 인터페이스와 비보안 인터페이스가 있어야 합니다. 구성 클라이언트 탐색 트리에서 시스템 관리 폴더를 열고 **인터페이스**를 눌러 Firewall에 있는 네트워크 인터페이스 목록을 봅니다. 인터페이스의 보안 상태를 변경하려면 인터페이스를 선택하고 **변경**을 누릅니다.
3. 시스템 관리 폴더에서 **보안 정책** 대화 상자를 액세스하여 일반 보안 정책을 설정합니다. 일반적인, Firewall 구성에 대해
   - DNS 조회를 허용합니다.
   - 비보안 인터페이스에 대한 브로드캐스트 메시지를 거부합니다.
   - 비보안 어댑터에 대한 Socks를 거부합니다.
4. 도메인 이름 서비스와 메일 서비스를 설정합니다. DNS 해상도를 제공하지 않으면 효율적인 통신이 이루어지지 않습니다. 구성 클라이언트 탐색 트리의 시스템 관리 폴더에서 이런 기능을 액세스합니다.
5. 구성 클라이언트 탐색 트리의 **네트워크 오브젝트** 기능을 사용하여 Firewall에서의 네트워크 주요 요소를 정의합니다. 네트워크 오브젝트는 Firewall을 통해 트래픽을 조절합니다. 다음 주요 요소를 네트워크 오브젝트로 정의하십시오.
   - Firewall의 보안 인터페이스

- Firewall의 비보안 인터페이스
- 보안 네트워크
- 보안 네트워크에서의 각 서브네트
- 해당하는 경우 Security Dynamics 서버와 Windows NT 도메인 서버에 대한 호스트 네트워크 오브젝트

6. Firewall에서 서비스를 사용할 수 있게 합니다. 이는 보안 네트워크에 있는 사용자가 비보안 네트워크를 액세스할 때 사용하는 메소드(예를 들어, socks 또는 프록시)입니다. 구현되는 서비스는 계획 단계에서 이루어지는 결정에 의해 달라집니다. 서비스를 구현할 때는 특정 유형의 트래픽을 허용하기 위해 일부 연결 구성을 설정해야 합니다. 예를 들어, 보안 사용자가 HTTP 프록시를 사용하여 인터넷의 웹을 탐색할 수 있게 하려면 Firewall의 HTTP 프록시 디먼을 구성할 뿐만 아니라 연결을 설정하여 HTTP 트래픽을 허용해야 합니다.
7. Firewall 사용자를 설정합니다. 아웃바운드 웹 액세스와 같은 기능이나 Firewall 관리자에 대한 인증이 필요하면 이런 사용자를 Firewall에서 정의해야 합니다. SecureWay Policy Director를 사용하여 프록시 사용자를 LDAP에 저장하는 경우 프록시 사용자를 작성하지 마십시오. Policy Director 콘솔을 사용하여 Policy Director 구성 중에 Firewall 프록시 사용자를 작성합니다.

이런 단계를 수행하면 기본 Firewall 구성이 시작되고 실행됩니다. IBM Firewall은 네트워크 보안을 확인할 수 있도록 시스템 로그와 같은 기타 기능을 제공합니다.

Firewall이 정상적으로나 비정상적으로 종료하는 경우 구성 데이터는 하드 드라이브에 저장되고 다시 부팅할 때 자동으로 재활성화되므로 영향을 받지 않습니다. 그러나, 활성화된 FTP 세션과 같은 일부 활성화된 연결이 인터럽트되었음을 알려주는 특정 Firewall 로그 메시지가 발생합니다.

Policy Director 통합을 위한 SecureWay Firewall 구성

Firewall은 Policy Director와의 통합을 활용하기 위해 IBM SecureWay Policy Director를 SecureWay Boundary Server 마법사와 함께 사용할 수 있도록 구성되어야 합니다. IBM SecureWay Policy Director가 사용되지 않으면 프록시 사용자는 Firewall 그래픽 사용자 인터페이스(GUI)만으로 정의됩니다. 이런 사용자는 SecureWay Policy Director에서 관리할 수 없습니다.

SecureWay Firewall은 SecureWay Directory와 통신할 수 있도록 연결이 이루어집니다. SecureWay Directory는 Firewall의 보안쪽인 보안 DMZ나 보안 네트워크에 있어야 합니다.

연결 설정에 대한 자세한 내용은 *IBM SecureWay Firewall User's Guide for Windows NT* 및 *IBM SecureWay Firewall User's Guide for AIX*를 참조하십시오. 연결 설정 정보는 다음과 같습니다.

요청에 대해 다음은 아웃바운드 규칙을 설정하는데 필요한 항목입니다.

- 소스는 Firewall의 보안 어댑터 주소가 됩니다.
- 대상은 SecureWay Directory 주소가 됩니다.
- 소스 포트는 1023보다 큽니다.
- 대상 포트는 389와 같습니다.
- 인터페이스는 보안이 됩니다.
- 라우팅은 로컬입니다.
- 방향은 아웃바운드입니다.

응답에 대해 다음은 인바운드 규칙을 설정하는데 필요한 항목입니다.

- 소스는 SecureWay Directory 주소가 됩니다.
- 대상은 Firewall의 보안 어댑터 주소가 됩니다.
- 소스 포트는 389와 같습니다.
- 대상 포트는 1023보다 큽니다.
- 인터페이스는 보안이 됩니다.
- 라우팅은 로컬입니다.
- 방향은 인바운드입니다.

연결 예제는 다음과 같습니다.

```
# 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
```

SecureWay Boundary Server 설정 마법사를 실행합니다. Firewall이 Policy Director와 함께 작업할 수 있도록 옵션을 선택합니다. 더 자세한 내용은 29 페이지의 『Policy Director 통합을 위한 SecureWay Boundary Server 구성』을 참조하십시오.

SurfinGate 플러그인을 사용하기 위한 SecureWay Firewall 구성 (Windows NT 전용)

SecureWay Firewall이 SurfinGate 서버와 통신할 수 있도록 연결이 이루어집니다. SurfinGate 서버는 Firewall의 보안쪽에 있어야 합니다.

연결 설정 방법에 대한 자세한 내용은 *IBM SecureWay Firewall User's Guide for Windows NT*를 참조하십시오. 연결 설정 정보는 다음과 같습니다.

요청에 대해 다음은 아웃바운드 규칙을 설정하는데 필요한 항목입니다.

- 소스는 Firewall의 보안 어댑터 주소가 됩니다.
- 대상은 SurfinGate 서버의 주소가 됩니다.
- 소스 포트는 1023보다 큽니다.
- 대상 포트는 3141과 같습니다.
- 인터페이스는 보안이 됩니다.
- 라우팅은 로컬입니다.
- 방향은 아웃바운드입니다.

요청에 대해 다음은 인바운드 규칙을 설정하는데 필요한 항목입니다.

- 소스는 SurfinGate 서버의 주소입니다.
- 대상은 Firewall의 보안 어댑터 주소가 됩니다.
- 소스 포트는 3141과 같습니다.
- 대상 포트는 1023보다 큽니다.
- 인터페이스는 보안이 됩니다.

- 라우팅은 로컬입니다.
- 방향은 인바운드입니다.

이런 연결 예제는 다음과 같습니다.

```
# 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
```

주: 연결은 같은 회선에 있어야 합니다.

또한, 스캔되는 데이터를 허용하도록 SurfinGate 서버를 구성해야 합니다. SurfinConsole(SurfinGate의 관리 인터페이스)에서 일반 탭 밑에 있는 **플러그인 모드** 옵션을 확인해야 합니다. 또한, Firewall의 HTTP 프록시의 주소와 포트 번호를 프록시 탭의 다음 프록시 필드에 입력해야 합니다.

MAILsweeper를 사용하기 위한 SecureWay Firewall 구성

SecureWay Fireewall에서 정의된 메일 교환기는 실제 보안 메일 서버 대신 MAILsweeper 시스템을 가리켜야 합니다. MAILsweeper 자체는 메일을 보안 메일 서버로 전달합니다.

SecureWay Policy Director 구성

SecureWay Directory가 설치되어 있는지 확인합니다. SecureWay Directory가 설치된 시스템의 주소, 청취 중인 포트, SecureWay Directory 서버에서의 관리자 ID 및 관리자 암호를 알고 있어야 합니다.

SecureWay Directory LDAP 클라이언트를 SecureWay Policy Director와 같은 시스템에 설치하십시오. (SecureWay Directory의 시스템과 같은 것을 사용하고 SecureWay Policy Director를 사용하는 경우 클라이언트는 이미 설치되어 있을 수도 있습니다.)

SecureWay Directory의 LDAP 계획을 수정하여 Policy Director eProxyUsers를 지원해야 합니다. 계획 추가는 Policy Director에서 제공하는 두 파일에 저장됩니다. Policy Director CD의 `/schema` 디렉토리에 위치한 `secschema.def`와 `puschema.def` 파일이 필요합니다.

SecureWay Directory 서버에서 LDAP 계획을 수정하려면 다음 명령을 Policy Director 시스템에서 실행하십시오.

```
ldapmodify -h <LDAPHOST> -p <LDAPPORT>  -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f secschema.def
ldapmodify -h <LDAPHOST> -p <LDAPPORT> -D <LDAPADMINUSER>  -w <LDAPADMINPWD>  -f puschema.def
```

여기서:

- <LDAPHOST>는 SecureWay Directory 서버 이름입니다
- <LDAPPORT>는 서버가 청취 중인 포트입니다
- <LDAPADMINUSER>는 관리자 ID입니다
- <LDAPADMINPWD>는 관리자 암호입니다

일단 LDAP 계획을 수정하여 프록시 사용자를 지원하면 Policy Director Console에 대해 프록시 사용자를 처리해야 합니다. 이렇게 하려면 \Program Files\IBM\IVConsole 디렉토리에 위치한 console.properties 파일에서 Proxyusers TaskView 줄을 주석 해제해야 합니다.

SecureWay Directory 구성

Policy Director 사용자가 저장되는 루트로 사용되는 SecureWay Director에서 접미사를 정의해야 합니다. LDAP에 접미사를 추가하려면 *IBM SecureWay Directory Administrator's Guide*를 참조하십시오. 예를 들어, 일반적인 접미사는 다음과 같습니다.

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

일단 Policy Director 사용자를 저장하기 위한 접미사를 추가하면 그 액세스 제어 목록(ACL)을 올바로 설정해야 합니다. Policy Director 보안 그룹에 대한 새 접미사에 모든 액세스 권한을 제공해야 합니다. Policy Director 보안 그룹에 대한 DN은 다음과 같습니다.

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

Policy Director 통합을 위한 SecureWay Boundary Server 구성

마법사를 사용하여 SecureWay Boundary 서버를 구성할 수 있습니다. 이 마법사는 Firewall이 Boundary Server에 있는 기타 제품 및 Policy Director와 함께 작업할 수 있도록 설정하는데 필요한 단계를 안내해 줍니다. 다음에 나오는 패널은

LDAP 서버에 대해 질문합니다. 필요한 모든 정보를 채운 경우 마법사는 Firewall을 설정하여 Policy Director가 사용자 및 그룹 정책에 사용하는 것과 같은 LDAP 데이터베이스를 사용하도록 합니다. 이 마법사는 또한 인증 정보를 SurfinGate 플러그인(Windows NT Firewall 전용)에 전달할 수 있도록 Firewall HTTP 프록시를 구성하거나 구성 해제합니다.

IBM SecureWay Boundary Server를 구성하려면 SecureWay Boundary Server 마법사를 구성하십시오. AIX에서 **sbswizard** 명령을 실행하여 Windows NT에서 **시작->프로그램->SecureWay Boundary Server**를 선택합니다. 이는 SBS 마법사를 불러옵니다.

1. 옵션을 선택하여 **Firewall이 Policy Director와 LDAP 데이터베이스를 공유하도록 설정합니다.**
2. 16 페이지의 『SecureWay Boundary Server』에 있는 정보를 사용하여 질문에 응답합니다.

SurfinGate 플러그인을 사용할 수 있도록 SecureWay Boundary Server 구성(Windows NT 전용)

시작->프로그램->SecureWay Boundary Server를 선택합니다. 이는 SBS 마법사를 불러옵니다.

1. 옵션을 선택하여 **인증 정보를 SurfinGate 플러그인으로 전달할 수 있도록 Firewall HTTP 프록시를 구성합니다.**
2. 대화를 완료합니다.

SurfinGate 구성

Windows NT에서 두 가지 방법으로 SurfinGate를 구성할 수 있습니다.

- 체인 프록시로
- Firewall HTTP 프록시의 플러그인으로

AIX에서 한 가지 방법으로 SurfinGate를 구성할 수 있습니다.

- 체인 프록시로

체인 프록시로 SurfinGate 구성

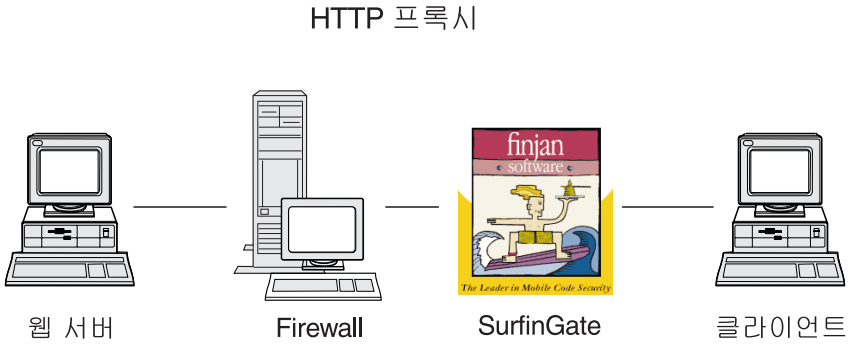

그림 2. SurfinGate 구성

클라이언트 웹 브라우저는 SurfinGate를 HTTP, FTP 그리고 HTTPS의 프록시로 사용할 수 있도록 구성되어야 합니다. SurfinGate가 청취 중인 포트 번호(기본값은 8080)를 반드시 지정하십시오.

SurfinConsole(SurfinGate의 관리 인터페이스)에서 일반 탭 밑에 있는 **프록시 모드** 옵션을 확인해야 합니다. 또한, Firewall의 HTTP 프록시의 주소와 포트 번호를 프록시 탭의 다음 프록시 필드에 입력해야 합니다. 또는 추가 프록시가 이미 정의된 경우 이를 다음 프록시로 지정할 수 있습니다.

Firewall HTTP 프록시에 대해 플러그인으로 SurfinGate 구성

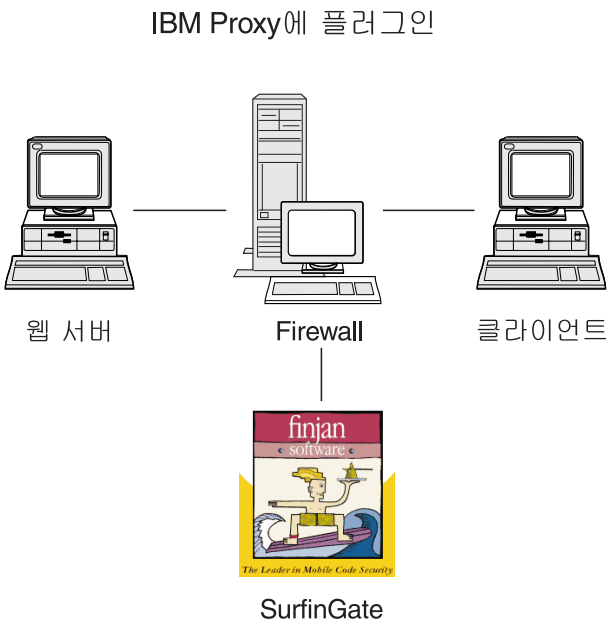

그림 3. SurfinGate 구성

클라이언트 웹 브라우저는 Firewall HTTP 프록시를 HTTP, FTP 그리고 HTTPS의 프록시로 사용할 수 있도록 구성되어야 합니다. Firewall HTTP 프록시가 청취 중인 포트 번호(기본값은 8080)를 지정하십시오.

SurfinConsole(SurfinGate의 관리 인터페이스)에서 일반 탭 밑에 있는 **플러그인 모드** 옵션을 확인해야 합니다. 또한, Firewall의 HTTP 프록시의 주소와 포트 번호를 프록시 탭의 다음 프록시 필드에 입력해야 합니다.

주: 이 기능은 Windows NT용 SecureWay Firewall에서만 사용할 수 있습니다.

MIMEsweeper 구성

MAILsweeper 구성

그림 4. MAILsweeper 구성

단순한 환경에서 MAILsweeper는 설치 중에 이루어지는 질문에 의해 구성되어야 합니다. 추가로 구성하려면 **시작->프로그램->SMTP용 MAILsweeper->SMTP 콘솔용 MAILsweeper**을 실행합니다. 더 자세한 내용은 *MAILsweeper Getting Started Guide*를 참조하십시오.

WEBsweeper 구성

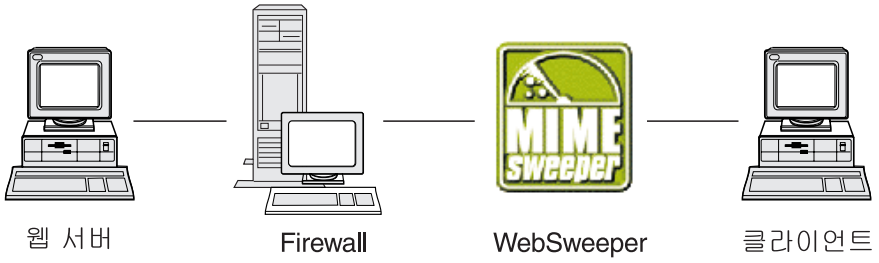

그림 5. WEBsweeper 구성

구성하려면 제어판으로 가서 WEBsweeper 애플릿을 선택합니다. 더 자세한 내용은 MIMEsweeper CD에 있는 *WEBsweeper Administrator's Guide*를 참조하십시오.

WEBsweeper HTTPS 구성

구성하려면 제어판으로 가서 WEBsweeper HTTPS 애플릿을 선택합니다. 더 자세한 내용은 *WEBsweeper Administrator's Guide*를 참조하십시오.

침입 차단

명령 행 유틸리티를 사용하여 특정 IP 주소를 차단할 수 있는 필터를 작성합니다. 차단되는 주소는 내용 조사 결과에 의해 동적으로 결정될 수 있습니다. 명령은 다음과 같습니다.

- fwadd_deny
- fwdelete_dynamic

fwadd_deny

프로그램이 매개변수 없이 호출되면 필요한 매개변수의 형식에 대한 프롬프트를 화면 표시합니다.

매개변수는 다음과 같습니다.

필터 ID

Windows NT Firewall에 대해 다음이 적용됩니다. ID는 유지보수를 구성하기 위해 필터에 할당될 수 있습니다. ID는 1에서 시작하여 오름차순으로 할당됩니다. 그리고 다음으로 사용할 수 있는 ID 번호보다 높은 ID가 제공되면 할당된 ID는 프로그램에 제공된 ID 번호가 아닌 다음으로 사용 가능한 ID 번호가 됩니다. 예를 들어, ID 1에 몇 가지 규칙이 있는데 ID 3로 필터 규칙 세트를 작성하려고 하면 ID 2가 대신 할당됩니다. 여러 규칙에 같은 ID 번호가 할당될 수 있습니다. delete_dynamic 프로그램을 사용하여 규칙이 삭제되면 이는 ID로 참조되므로 ID로 규칙을 작성할 때는 이 규칙들이 같은 ID를 공유하는 경우 이를 그룹으로 삭제하십시오.

규칙이 추가되면 사용된 ID 번호가 표시됩니다.

필터 ID

AIX Firewall에 대해 다음이 적용됩니다. ID는 번호로 할당될 수 있습니다. 예를 들어, 필터 id가 ID 12일 경우 이는 ID=12로 할당됩니다. AIX에는 같은 ID 번호로 할당된 필터가 없습니다. 각 필터는 각각 고유한 ID가 있습니다.

소스 IP 주소

패킷 소스에 사용할 IP 주소는 255.255.255.255와 같은 점분리 십진 표기법으로 입력되어야 합니다.

소스 IP 마스크

이 필드는 소스 IP 주소와 함께 사용되어야 하고 점분리 십진 표기법으로 입력됩니다. 예를 들어, 소스 IP 주소가 10.5.8.0으로 입력되고 소스 IP 마스크가 255.255.255.0이면 10.5.8.1에서 10.5.8.255까지의 모든 패킷이 일치됩니다.

대상 IP 주소

패킷 대상에 사용할 IP 주소는 255.255.255.255와 같은 점분리 십진 표기법으로 입력되어야 합니다.

대상 IP 마스크

이 필드는 대상 IP 주소와 함께 사용되며 점분리 십진 표기법으로 입력됩니다. 예를 들어, 대상 IP 주소가 10.5.8.0으로 입력되고 대상 IP 마스크가 255.255.255.0이면 10.5.8.1에서 10.5.8.255까지의 모든 패킷이 일치됩니다.

어댑터 어댑터 스펙은 다음과 같습니다.

S 보안으로 지정된 어댑터에 대해

N 비보안으로 지정된 어댑터에 대해

B 모든 어댑터에 대해(보안 및 비보안)

지정된 유형에 맞는 어댑터(들)에서 시작한 패킷은 규칙과 일치합니다.

유효 범위

Firewall을 통한 패킷 트래버설의 유효 범위는 다음 값 중 하나가 될 수 있는 이 매개변수로 지정됩니다.

L 로컬 패킷에 대해

R 경로 지정된 패킷에 대해

B 로컬과 경로 지정된 패킷에 대해

방향 인바운드, 아웃바운드 또는 양쪽 방향으로 진행하는 트래픽을 지정합니다.

I 인바운드 트래픽에 대해

O 아웃바운드 트래픽에 대해

B 인바운드와 아웃바운드 트래픽에 대해

기록 동적 필터 활동에 대해 기록하려면 Y를 지정하고 기록하지 않으려면 N을 지정합니다.

fwdelete_dynamic

이 프로그램이 매개변수 없이 호출되면 현재 정의된 모든 동적 필터가 표시됩니다.

```
>>>>  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
```

주: fwdelete_dynamic 명령을 사용하여 삭제되어야 하는 규칙에 예상 ID가 있는지를 먼저 확인합니다.

프로그램이 유효한 필터 ID와 함께 호출되면 동적 규칙은 삭제되고 삭제된 규칙의 수는 id가 있는 x 규칙 발견: x의 형식으로 표시됩니다.

경고: 중복 필터를 추가하려고 하면 필터가 이미 있다는 것을 알려줍니다. 필터 ID 없이 필터를 추가하려고 하면 경고 오류를 받게 됩니다.

: AIX 침입 차단은 상위 레벨 규칙 세트에 규칙이 있으면 겹쳐쓰여질 수 있습니다.
: 침입 차단이 사용되면 대부분의 규칙은 하위 레벨 규칙 세트에 있어야 합니다. 동
: 적 규칙은 이런 두 규칙 세트 중간에 추가됩니다. 트래픽을 허용하는 규칙이 상위
: 레벨에 있으면 동적 규칙으로 트래픽을 작동 중지시킬 수 없습니다.

구성 테스트

이전 창에서 모든 설정을 완료한 후 그 설정을 테스트해야 합니다. SecureWay Boundary Server의 구성을 테스트하려면 다음을 수행하십시오.

1. Policy Director를 사용하여 Firewall 프록시 사용자를 설정합니다. 사용자가 보안 텔넷에 대해 Firewall 암호를 사용하도록 설정하고 그 사용자에 대해 암호를 설정합니다.
2. SecureWay Boundary Server 마법사를 실행하여 Firewall과 Directory(LDAP) 간에 링크를 설정합니다.
3. 보안 클라이언트에서 프록시 텔넷 세션을 시작합니다.
4. 사용자 설정을 Policy Director에 입력합니다.
5. 암호를 입력합니다.
6. 이제 사용자는 인증됩니다.

제6장 관련 문서

본 장에 있는 문서를 사용하여 IBM SecureWay Boundary Server 버전 2.0과 그 관련 제품에 대해 더 많은 정보를 얻을 수 있습니다.

IBM SecureWay FirstSecure

다음 *IBM SecureWay FirstSecure 계획 및 통합, 버전 2.0*에는 FirstSecure에 대한 정보가 들어 있습니다. 이 책은 FirstSecure를 구성하고 모든 IBM SecureWay 제품 사용을 계획할 수 있도록 도와주는 제품을 설명합니다.

IBM SecureWay Firewall

다음 문서에는 Windows NT용 IBM SecureWay Firewall에 대한 정보가 들어 있으며 IBM SecureWay Firewall CD의 `x:\books\en_US` 디렉토리에서 PDF와 HTM 형식으로 사용할 수 있습니다.

- *IBM SecureWay Firewall for Windows NT Setup and Installation*
- *IBM SecureWay Firewall for Windows NT User's Guide*
- *IBM SecureWay Firewall for Windows NT Reference*
- *Guarding the Gates Using the IBM eNetwork Firewall for Windows NT 3.3* (redbook)

다음 문서에는 AIX용 IBM SecureWay Firewall에 대한 정보가 들어 있으며 IBM SecureWay Firewall CD의 `books/en_US` 디렉토리에서 PDF와 HTM 형식으로 사용할 수 있습니다.

- *IBM SecureWay Firewall for AIX Setup and Installation*
- *IBM SecureWay Firewall for AIX User's Guide*
- *IBM SecureWay Firewall for AIX Reference*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (redbook)

MIMEsweeper

MAILsweeper

다음 문서에는 MAILsweeper에 대한 정보가 들어 있으며 MIMEsweeper CD의 \install에서 PDF와 HTM 형식으로 사용할 수 있습니다.

- *Getting Started Guide*는 \install\MSW4_0_2\Doc\qsg.pdf에 있습니다
- Readme는 \install\MSW4_0_2\README.htm에 있습니다

WEBsweeper

다음 문서에는 WEBsweeper에 대한 정보가 들어 있으며 MIMEsweeper CD의 \install에서 PDF와 HTM 형식으로 사용할 수 있습니다.

- *WEBsweeper Administrator's Guide*는 \install\WSW3_2_5\Doc\manual.pdf에 있습니다
- 릴리스 정보는 \install\WSW3_2_5\Doc\RELNOTES.htm에 있습니다

WEBsweeper HTTPS 프록시

다음 문서에는 WEBsweeper HTTP 프록시에 대한 정보가 들어 있으며 MIMEsweeper CD의 \install에서 TXT 형식으로 사용할 수 있습니다.

- Readme는 \install\WSWHTTPS1_0_2\readme.txt에 있습니다

SurfinGate

다음 문서에는 SurfinGate에 대한 정보가 들어 있으며 SurfinGate CD의 \docs에서 PDF 형식으로 사용할 수 있습니다.

- *SurfinGate Installation Guide*는 \Docs\install.pdf에 있습니다
- *SurfinGate User's Manual*은 \Docs\manual.pdf에 있습니다
- 릴리스 정보는 \Docs\SFG 405 RelNotes.pdf에 있습니다
- SurfinGate 플러그인에 대한 정보는 \docs 디렉토리에 있습니다.

부록A. 문제 해결

본 장에서는 SecureWay Boundary Server에 관련된 문제를 발견하고 해결하는 데 도움을 줍니다.

IBM SecureWay Firewall의 공통 문제 해결

경로 지정 문제

IBM Firewall은 경로 지정 문제를 디버그하는데 도움이 될 수 있는 *IP 경로 지정 테스트*라고 되어 있는 **Security Policy** 대화 상자에 기능을 제공합니다. 이 선택란을 사용할 수 있게 하고 연결 구성을 활성화하며 연결 규칙 기록을 사용합니다. 그런 후 `Firewall` 로그를 조사하여 Firewall을 통과하는 모든 패킷에 대한 상세한 정보를 봅니다.

IP 주소를 사용한 후 호스트 이름을 사용하여 먼저 이런 테스트를 수행하십시오.

Firewall에서 호스트를 Ping할 수 없습니다

문제 설명

네트워크 인터페이스가 제대로 구성되어 있지 않습니다.

권장 조치

운영 체제 문서를 참조하십시오.

문제 설명

비보안 네트워크에 대한 연결이 제대로 구성되지 않았습니다.

권장 조치

인터넷 서비스 제공자에게 지원을 요청하십시오.

문제 설명

보안 네트워크가 라우터 뒤에 격리되어 있으면 Firewall에는 그 라우터에 대한 정적 경로가 있어야 합니다. `netstat -rn`을 사용하여 정적 경로 지정을 확인하십시오.

```
netstat -rn
```

출력은 프로토콜 패밀리 2에 대해 다음과 같아야 합니다.

```
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
```

그림 6. netstat -rn의 예제 출력.

nrr.nrr.nrr.nrr

인터넷에 대한 라우터를 나타내고 이는 기본 경로입니다. 기본 경로는 정적 경로(플래그=UG)입니다.

nnn.nnn.nnn

비보안 도메인을 나타냅니다. 이는 인터페이스 경로(플래그=U)입니다.

nnn.nnn.nnn.nnn

비보안 인터페이스를 나타냅니다.

sss.sss.sss

보안 도메인을 나타냅니다. 이는 인터페이스 경로(플래그=U)입니다.

sss.sss.sss.sss

보안 인터페이스를 나타냅니다.

ss1.ss1.ss1

네트워크의 보안쪽의 서브 도메인을 나타내고 srr.srr.srr.srr은 그 서브 도메인에 대한 라우터를 나타냅니다. 이는 정적 경로(플래그=UG)입니다.

127.0.0.1

루프백이거나 로컬 호스트입니다. 이는 인터페이스 경로(플래그=U)입니다.

각 인터페이스에 대해 인터페이스 경로가 있어야 하고 기본 경로는 Firewall의 비보안쪽에 있는 라우터를 가리켜야 합니다.

권장 조치

정적 경로를 라우터에 추가하십시오. 라우터 관리자에게 문의하십시오. `route add` 명령을 사용합니다.

문제 설명

보안 인터페이스에 있는 서브네트 마스크나 접속하려는 호스트가 틀릴 수 있습니다.

권장 조치

클라이언트 구성 유틸리티를 사용하여 마스크 설정을 정정하십시오.

보안 호스트에서 비보안 호스트를 Ping할 수 없습니다(또는 그 반대)

문제 설명

Firewall에 인접해 있는 각 라우터에는 Firewall 뒤에 있는 대상 네트워크의 게이트웨이로 Firewall을 지정하는 정적 경로가 있어야 합니다.

권장 조치

라우터의 관리자에게 문의하십시오.

문제 설명

보안 네트워크에서 RFC 1597에 지정된 개인 주소를 포함하여, 미등록이고 비보안 네트워크에서 경로 지정할 수 있는 주소를 사용하는 경우 패킷은 전송자에게 다시 경로 지정되지 않습니다.

권장 조치

Windows NT 전용: 클라이언트를 등록된 주소와 함께 사용하십시오. Firewall의 NAT 기능은 TCP 및 UDP 트래픽에 사용될 수 있지만 NAT는 ICMP 패킷에서 주소를 ping처럼 변환하지 않습니다.

권장 조치

AIX 전용: 클라이언트를 등록된 주소와 함께 사용하십시오.

DNS 실패

주: DNS는 Windows NT 전용이 아닙니다.

문제 설명

Microsoft DNS 서비스를 Microsoft DNS 서비스 관리자로 구성했으므로 DNS 오류 메시지를 수신했습니다.

권장 조치

설치 지침을 다시 참조하고

1. 전체 디렉토리인 \winnt\system32\DNS를 삭제하여 Microsoft DNS를 제거합니다.
2. Microsoft DNS를 다시 설치합니다.
3. 다시 부트합니다.
4. DNS hotfix를 다시 설치합니다.
5. 다시 부트합니다.

공통 문제–MIMEsweeper 해결

WEBsweeper 및 MAILsweeper는 같은 시스템에서 작동하지 않는 것 같습니다

문제 설명

MAILsweeper와 WEBsweeper를 같은 시스템에서 실행하려고 할 때 문제가 발생합니다.

권장 조치

MAILsweeper와 WEBsweeper를 서로 다른 시스템에 설치하십시오.

WEBsweeper의 저하된 성능

문제 설명

WEBsweeper를 사용하여 웹 내용을 다운로드할 때 만족스럽지 못하게 지연됩니다.

권장 조치

1. WEBsweeper 제어판 애플릿을 사용하여 기록하지 못하게 합니다.

2. WEBsweeper를 사용할 수 있는 하드웨어 중 가장 빠른 것에 설치합니다.

WEBsweeper 라이센스 문제

문제 설명

WEBsweeper 3.2_5를 WEBsweeper의 이전 버전이 설치된 시스템에 설치한 경우 라이센스 키 충돌이 발생할 수 있습니다. WEBsweeper가 시작될 때 내부 Windows 오류 메시지: 2140이 발생하면 이벤트 표시기에서 응용 프로그램 로그를 확인합니다. WEBsweeper의 메시지는 다음과 같습니다. ″PAKMSG 오류: 사용자 이름은 이전에 정의된 라이센스 섹션과 충돌합니다.″

권장 조치

Windows 레지스트리에서 이전 라이센스 키를 제거하십시오. Regedit를 찾아보고 \\HKEY_LOCAL_MACHINE\SOFTWARE\Content Technologies\MIMEsweeper\License 경로에서 찾아보십시오. 여기서 키를 하나 이상 찾으면, ″IBM MIMEsweeper System″으로 레이블이 붙지 않은 것을 삭제하십시오. 다시 부트합니다.

WEBsweeper는 규모가 큰 파일을 다운로드할 때 문제가 발생합니다

문제 설명

WEBsweeper는 필터링하는 중에 파일을 저장하기 위한 가상 메모리가 부족할 수 있습니다.

권장 조치

WEBsweeper 서버에서 실제 메모리량을 늘리십시오.

공통 문제—SurfinGate 해결

SurfinConsole은 Microsoft Internet Explorer가 열려 있는 동안에는 응답하지 않습니다

문제 설명

SurfinConsole 응용 프로그램은 Internet Explorer가 열려 있는 동안 이상한 동작을 보이거나 응답하지 않습니다. 이런 두 응용 프로그램은 충돌하므로 동시에 실행할 수 없습니다.

권장 조치

Internet Explorer와 SurfinConsole을 동시에 로드하지 마십시오.

SurfinGate 플러그인의 저하된 성능

문제 설명

웹을 통한 모빌 코드 다운로드는 SurfinGate 플러그인을 사용할 때 매우 느립니다.

권장 조치

다음 프록시 필드는 SurfinConsole의 프록시 섹션에서 SecureWay Firewall HTTP 프록시로 설정되어야 합니다.

부록B. 주의사항

이 책에서 IBM 제품, 프로그램 또는 서비스를 참조했다고 해서 IBM이 영업 중인 모든 나라에서 이를 사용할 수 있다는 것을 의미하지는 않습니다. 이 책에서 IBM 사용권 프로그램 또는 IBM 제품을 언급했다고해서 반드시 IBM 프로그램이나 제품만이 사용되어야 함을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한 기능적으로 동등한 제품,프로그램 또는 서비스를 IBM 제품, 프로그램 또는 서비스 대신 사용할 수 있습니다. IBM이 특별히 명시하지 않는 다른 제품과 관련된 조작의 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에 나오는 특정 항목에 대한 특허를 보유하고 있거나 현재 출원 중일 수 있습니다. 이 책을 제공한다고 해서 그 특허에 대한 사용권까지 부여하는 것은 아닙니다. 특허 사용권에 대해서는 다음 주소로 서면 문의하십시오.

150-010
서울특별시 영등포구 여의도동 25-11, 한진해운빌딩
한국 아이.비.엠 주식회사
지적 재산권부

(i)별도로 작성된 프로그램과 기타 프로그램(이 프로그램을 포함한) 간의 정보 교환 및 (ii)교환된 정보의 상호 이용을 목적으로 이에 대한 정보를 원하는 사용권자는 다음 주소로 문의하십시오.

150-010
서울특별시 영등포구 여의도동 25-11, 한진해운빌딩
한국 아이.비.엠 주식회사
소프트웨어 사업본부

IBM 고객 계약(ICA) 하에 프로그램의 사용권이 부여되지 않습니다. 이는 IBM 국제 프로그램 사용권 계약(IPLA) 하에 사용권이 부여됩니다.

이 책은 생산용이 아니며 상업성 또는 특정 목적에 대한 타당성에 대한 보증을 포함하여 어떠한 종류의 보증도 제공하지 않고 현상대로 이 책을 제공합니다.

이 제품에는 CERN에서 작성하고 사용할 수 있게 만들어진 컴퓨터 소프트웨어가 들어 있습니다. 이 승인은 CERN 컴퓨터 소프트웨어가 포함된 모든 제품에서 자세히 언급되어야 합니다.

등록상표

다음 용어는 미국이나 기타 국가에서 사용되는 IBM 사의 등록상표입니다.

AIX

IBM

Microsoft와 Windows NT는 Microsoft의 상표 또는 등록상표입니다.

**SurfinGate는 Finjan Software의 상표입니다.

**MIMEsweeper, **MAILsweeper 그리고 **WEBsweeper는 Content Technologies의 상표입니다.

별표가 두 개(**) 표시된 기타 회사, 제품 및 서비스명은 다른 회사의 등록상표나 서비스 상표입니다.

용어

가

게이트웨이(gateway). 서로 다른 구조의 두 컴퓨터 네트워크를 상호 연결하는 기능적 장치.

기본값(default). 명시적으로 지정된 것이 없는 경우 간주되는 값, 속성 또는 옵션.

라

루프백 인터페이스(loopback interface). 정보의 주소가 동일한 시스템의 엔티티로 지정된 경우 불필요한 통신 기능을 생략하는 인터페이스입니다.

마

마법사(wizard). 사용자가 특정 작업을 진행해 나갈 수 있도록 단계별 지침을 사용하는 응용 프로그램의 대화입니다.

사

서버 주소(server address). 네트워크를 통해 파일 서버, 인쇄 서버 또는 메일 서버와 같은 기타 컴퓨터에 공유 서비스를 제공하는 각 컴퓨터에 할당된 고유한 코드. 표준 IP 주소는 32 비트 주소 필드입니다. 서버 주소는 점분리 십진 IP 주소이거나 호스트 이름일 수 있습니다.

서버(server). 네트워크를 통해 다른 컴퓨터에 공유 서비스를 제공하는 컴퓨터. 예를 들어, 파일 서버, 인쇄 서버 또는 메일 서버 등이 있습니다.

서비스(service). 예를 들어, HTTP, FTP 또는 텔넷과 같은 하나 이상의 노드에서 제공하는 기능입니다.

쉘(shell). 사용자 워크스테이션에서 명령 행을 받아들이고 처리하는 소프트웨어. Korn 쉘은 사용 가능한 여러 UNIX 쉘 중 하나입니다.

시간초과(timeout). 조작이 실행될 수 있도록 할당된 시간 간격입니다.

아

웹(Web). 대부분은 HTTP 서버의 기타 문서에 대한 링크가 들어 있는 하이퍼텍스트 문서인 프로그램과 파일이 있는 HTTP 서버의 네트워크입니다. 월드 와이드 웹(World Wide Web)이라고도 합니다.

인터넷(Internet). 인터넷 프로토콜 그룹을 사용하고 공용 액세스를 허용하는 전 세계적으로 서로 연결된 네트워크의 컬렉션.

인트라넷(intranet). 인터넷 표준과 응용 프로그램(예를 들어, 웹 브라우저)을 조직의 기존 컴퓨터 네트워킹 하부구조와 통합하는 사설 보안 네트워크.

카

클라이언트(client). 일반적으로 서버라고 하는 또 다른 컴퓨터 시스템이나 프로세스의 서비스를 요청하는 컴퓨터 시스템 또는 프로세스. 여러 클라이언트는 공통 서버에 대한 액세스를 공유할 수 있습니다.

타

텔넷(Telnet). 터미널 에뮬레이션 프로토콜로서 원격 연결 서비스에 대한 TCP/IP 응용 프로그램 프로토콜입니다. 텔넷을 통해 한 사이트에 있는 사용자는 마치 사용자의 워크스테이션이 원격 호스트에 직접 연결된 것처럼 그 호스트를 액세스할 수 있습니다.

파

포트(port). 추상적인 통신 장치를 식별하는 번호. 웹 서버는 기본적으로 포트 80을 사용합니다.

프로토콜(protocol). 통신이 이루어지는 경우 통신 시스템의 기능적 단위의 조작을 관리하는 규칙 세트. 프로토콜은 바이트의 비트가 전송되는 순서와 같은 시스템 간 인터페이스의 하급 세부사항을 결정할 수 있습니다. 이는 또한 파일 전송과 같은 응용 프로그램 간 상급 교환을 결정할 수 있습니다.

D

DMZ. Demilitarized Zone. 외부 사용자가 회사 데이터가 들어 있는 서버를 직접 액세스하지 못하게 하는 장치.

F

Firewall. 하나의 네트워크와 다른 네트워크 간에 연결을 보호하고 제어하는 기능적 장치. Firewall은 원하지 않거나 권한이 부여되지 않은 통신 트래픽이 보호된 네트워크에 들어오지 못하도록 막고 선택된 통신 트래픽만 보호된 네트워크에서 나올 수 있도록 합니다.

FTP(File Transfer Protocol). 파일을 네트워크 컴퓨터와 주고 받을 때 사용하는 응용 프로그램 프로토콜. FTP는 사용자 ID가 필요하고 때때로 원격 호스트 시스템에 있는 파일에 대한 액세스를 허용하기 위해 암호가 필요합니다.

I

ICMP. (Internet Control Message Protocol). 인터넷 프로토콜(IP) 계층에서 오류와 제어 메시지를 처리할 때 사용하는 프로토콜. 문제 보고와 잘못된 데이터그램 대상은 원래 데이터그램 소스로 리턴됩니다.

IP. (Internet Protocol). 네트워크나 상호 연결된 네트워크에서 데이터를 연결 없이 경로 지정하는 프로토콜. IP는 더 높은 프로토콜 계층과 실제 계층 간에 중간 역할을 합니다.

IP 주소(IP address). 인터넷 프로토콜 주소. 네트워크에서 각 장치나 워크스테이션의 실제 위치를 지정하는 고유한 32 비트 주소. 이는 또한 인터넷 주소라고도 합니다.

IPSEC. (Internet Protocol Security). 네트워크나 네트워크 통신의 패킷 처리 계층에서 개발 중인 보안 표준입니다.

N

NAT. (Network Address Translation). Firewall에서 보안 IP 주소를 등록된 외부 주소로 변환하는 것. 이를 통해 외부 네트워크와 통신할 수 있지만 Firewall 내부에서 사용되는 IP 주소를 마스크합니다.

P

PICS. (Platform for Internet Content Selection). PICS를 사용할 수 있는 클라이언트는 사용자가 사용할 등급 서비스를 결정하고 각 등급 서비스에서 허용할 수 있는 등급과 허용할 수 없는 등급을 결정할 수 있게 합니다.

Ping. 응답을 받을 것으로 기대하면서 ICMP 에코 요청 패킷을 호스트, 게이트웨어 또는 라우터로 전송하는 명령.

S

SMTP. (Simple Mail Transfer Protocol). 인터넷 프로토콜 그룹에서 인터넷 환경에 있는 사용자 간에 메일을 전송할 때 사용하는 응용 프로그램 프로토콜입니다. SMTP는 메일 교환 순서와 메시지 형식을 지정합니다. 이는 TCP(Transmission Control Protocol)를 기초 프로토콜로 간주합니다.

T

TCP. (Transmission Control Protocol). 인터넷에서 사용되는 통신 프로토콜입니다. TCP는 신뢰할 수 있는 호스트 간 정보 교환을 제공합니다. 이는 IP를 기초 프로토콜로 사용합니다.

TCP/IP. (Transmission Control Protocol/Internet Protocol). 각 네트워크에서 사용하는 통신 기술에 관계없이 네트워크 간에 통신할 수 있게 설계된 프로토콜 그룹입니다.

U

UDP. (User Datagram Protocol). 인터넷 프로토콜 그룹에서 신뢰할 수 없는 단절된 데이터그램 서비스를 제공하는 프로토콜입니다. 이를 통해 한 시스템에 있는 프로그램이나 프로세스는 데이터그램을 다른 시스템에 있는 응용 프로그램이나 프로세스로 전송합니다. UDP는 IP를 사용하여 데이터그램을 전달합니다.

V

VPN. (Virtual Private Network). 두 개 이상의 네트워크를 연결하는 하나 이상의 보안 IP 터널로 구성된 네트워크입니다.

W

WTE. (Web Traffic Express). 매우 효율적인 캐시 계획을 통해 일반 사용자의 응답 시간을 가속화하는데 도움을 줄 수 있는 캐시 프록시 서버입니다. 유연한 PICS 필터링은 네트워크 관리자가 하나의 중앙 위치에서 웹 기반 정보에 대한 액세스를 제어할 수 있도록 도와 줍니다.

IBM 한글 지원에 관한 설문

FAX : (02) 781-7778

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다.
독자 여러분의 좋은 의견을 기다립니다.

책 제목: Windows NT 및 AIX용 IBM SecureWay Boundary Server 시작에서 수행까지 버전 2.0

책 번호: GA30-1012-00

성 명		직위/담당업무	
회 사 명		부 서 명	
주 소			
전화번호		팩스번호	
전자우편 주소			
사용중인 시스템	☐ 중대형 서버 ☐ UNIX 서버 ☐ PC 및 PC 서버		

1. IBM에서 제공하는 한글 책자와 영문 책자 중 어느 것을 더 좋아하십니까? 그 이유는 무엇입니까?
   ☐ 한글 책자 ☐ 영문 책자
   (이유:)

2. 본 책자와 해당 소프트웨어에서 사용된 한글 용어에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

3. 본 책자와 해당 소프트웨어에서 번역 품질에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

4. 본 책자의 인쇄 상태에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

5. 한글 소프트웨어 및 책자가 지원되는 분야에 대해 귀하는 어떻게 생각하십니까?
   ☐ 한글 책자를 늘려야 함 ☐ 현재 수준으로 만족
   ☐ 그다지 필요성을 느끼지 않음

6. IBM은 인쇄물 형식(hardcopy)과 화면 형식(softcopy)의 두 종류로 책자를 제공합니다. 어느 형식을 더 좋아하십니까?
   ☐ 인쇄물 형식(hardcopy) ☐ 화면 형식(softcopy) ☐ 둘 다

IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

☺ 설문에 답해 주셔서 감사합니다.
귀하의 의견은 저희에게 매우 소중한 것이며, 고객 여러분들께 보다 좋은 제품을 제공해 드리기 위해 최선을 다하겠습니다.

부품 번호: CT6RZKO

Printed in Singapore

GA30-1012-00

CT6RZKO

Spine information:

IBM

Windows NT® 및 AIX용
IBM SecureWay®
Boundary Server

시작에서 수행까지

버전 2.0