IBM® SecureWay® FirstSecure

계획 및 통합

버전 2

IBM® SecureWay® FirstSecure

계획 및 통합

버전 2

주

이 정보와 여기서 지원하는 제품을 사용하기 전에 107 페이지의 『부록. 주의사항』에 있는 일반 정보를 읽으십시오.

초판(1999년 10월)

이 개정판은 새 개정판에서 달리 언급하지 않는 이상 IBM SecureWay FirstSecure 버전 2와 모든 후속 릴리스 및 수정판에 적용됩니다.

목차

그림

표

이 책에 대하여

FirstSecure로도 알려진 IBM® SecureWay® FirstSecure는 회사에서 다음과 같은 작업을 수행할 수 있도록 도와주는 포괄적인 프레임워크입니다.

- 웹과 기타 네트워크를 통하는 네트워킹의 모든 측면을 보안합니다.
- 현재 e-business 투자 위에 구축합니다. 모듈 방식은 계획된 전개에 보안을 추가할 수 있게 합니다.
- 보안 e-business를 관리하기 위한 소유권 총 비용을 줄입니다.

이 책은 FirstSecure, FirstSecure를 구성하는 제품에 대해 설명하고 제품 사용을 계획할 수 있도록 합니다.

이 책에서 설명하는 제품은 단계별로 진행 중인 릴리스의 일부입니다. 모든 나라에서 동시에 모든 제품을 사용할 수 있는 것은 아닙니다. 이런 제품을 사용할 수 있는지에 대해서는 IBM 마케팅 대표부에 문의하십시오.

이 책에 있는 그림

이 책에 있는 그림은 계획용으로만 사용됩니다. 각 그림은 수 많은 서버, 클라이언트 및 응용 프로그램의 배열 중에서 사용자의 조직에 적합한 것 하나를 보여줍니다.

그림의 형식은 책의 전달 방법에 따라 달라집니다.

- 책의 PDF(Portable Document Format) 버전으로 되어 있는 대부분의 그림은 디스크 공간을 더 쉽게 절약하고 더 빨리 인쇄할 수 있습니다.
- 인쇄판에 있는 그림은 더 복잡하고 더 많은 저장영역을 차지하며 인쇄 시간이 더 오래 걸립니다.

양 버전에 있는 그림은 기능적으로 동등하고 동일한 캡션과 대체 텍스트가 있습니다.

이 책의 사용자

이 책은 웹 기반 시스템에서 보안을 계획하고 통합하려는 시스템 관리자를 위한 것입니다. 사용자는 사용 중인 네트워크와 e-business 응용 프로그램에 대해 미리 이해하고 있어야 합니다.

이 책의 구성

이 책은 다음으로 구성되어 있습니다.

- 1 페이지의 『제1부 FirstSecure 개요』에서는 FirstSecure 개요, 그 구성 제품 및 사용 가능한 자원에 대해 설명합니다
- 17 페이지의 『제2부 보안 e-business 네트워크 계획』에서는 보안 e-business 네트워크에 대한 계획을 설명합니다.
- 59 페이지의 『제3부 설치 및 통합 고려사항』은 FirstSecure 제품의 설치 요구사항과 통합 세부사항에 대해 설명합니다.
- 93 페이지의 『제16장 FirstSecure에서 제공하는 문서』는 FirstSecure와 함께 사용할 수 있는 모든 문서를 설명합니다.
- 111 페이지의 『용어』은 이 책에서 사용되는 보안 관련 용어를 정의합니다.

책에는 또한 각 제품의 문서를 설명하는 관련 서적 목록이 있습니다.

2000년 대비

IBM SecureWay FirstSecure 대비는 아래에 설명되어 있습니다.

IBM SecureWay FirstSecure에 있는 IBM 제품

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

기타 공급업체 제품

IBM에 제공된 기타 제품은 2000년에 대한 준비가 되어 있습니다. 그러나, IBM은 이런 제품을 설명하거나 그 제품의 2000년 대비를 보증하지 않습니다. 이런 제품의 2000년 대비에 대해서는 제조업체에 문의하십시오. IBM 이외의 제품과 서비스에 관한 정보는 다른 회사에서 제공하는 제품과 서비스에 대한 정보를 기반으로 한 Information and Readiness Disclosure Act의 ″재판물″입니다. IBM에 제공된 이런 제품은 2000년에 대한 준비가 되어 있습니다. 그러나, IBM은 이런 제품을 설명하거나 그 제품의 2000년 대비를 보증하지 않습니다. 이런 제품의 2000년 대비에 대해서는 제조업체에 문의하십시오. IBM은 이런 재판물의 내용을 독립적으로 확인하지 않으면 이런 재판물에 들어 있는 정보의 완벽성에 대해 책임을 지지 않습니다.

서비스 및 지원

SecureWay FirstSecure에서 제공하는 내용에 들어 있는 모든 제품에 대한 서비스와 지원에 대해서는 IBM에 문의하십시오. 이런 제품 중 일부는 IBM 이외의 지원이 필요합니다. 이런 제품을 SecureWay FirstSecure에서 제공하는 것의 일부로 받는 경우 IBM에 문의하여 서비스와 지원을 받으십시오.

용례

이 책은 다음과 같은 인쇄 규칙을 사용합니다.

- **굵은체**는 선택한 항목 이름, 명령 이름, 사용자가 입력한 텍스트 또는 실행 중인 텍스트에 있는 예제를 나타냅니다.
- 모노스페이스 유형은 예제(임시 경로 이름 또는 파일 이름) 또는 화면에 표시되는 텍스트를 나타냅니다.

웹 정보

FirstSecure의 최신 갱신에 대한 정보는 다음 위치의 인터넷 www.ibm.com/software/security에서 얻을 수 있습니다.

IBM SecureWay FirstSecure

www.ibm.com/software/security/firstsecure

문서는 www.ibm.com/software/security/firstsecure/library에서 얻을 수 있습니다.

IBM SecureWay Policy Director

www.ibm.com/software/security/policy

문서는 www.ibm.com/software/security/policy/library에서 얻을 수 있습니다.

IBM SecureWay Boundary Server

www.ibm.com/software/boundary

문서는 www.ibm.com/software/boundary/library에서 얻을 수 있습니다.

IBM SecureWay Trust Authority

www.ibm.com/software/security/trust

문서는 www.ibm.com/software/securitytrust/library에서 얻을 수 있습니다.

ITSO redbook인 *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498–00은 인터넷의 www.ibm.com/redbooks에서 얻을 수 있습니다.

제1부 FirstSecure 개요

이 부분은 FirstSecure와 그 구성요소 제품에 대한 개요입니다. 여기에는 각 제품에 대한 간단한 설명이 들어 있습니다.

이 부분은 또한 IBM 구현 서비스를 설명합니다.

제1장 FirstSecure 정의

IBM SecureWay FirstSecure는 IBM의 통합된 보안 솔루션의 일부입니다. FirstSecure는 회사에서 다음과 같은 작업에 도움을 주는 포괄적인 구축 블록 세트입니다.

- 보안 e-business 환경을 설정합니다.
- 보안 계획 과정을 단순화하여 보안 소유권의 총 비용을 줄입니다.
- 보안 정책을 좀 더 쉽게 구현합니다.
- 더 효과적인 e-business 환경을 만듭니다.

FirstSecure 구성요소에는 바이러스 보호, 침입 감지, 액세스 제어, 트래픽 내용 제어, 암호화, 디지털 인증서, Firewall 기술 및 응용 프로그램 개발 툴킷이 있습니다. 이런 기능은 여러 보안 공급업체 중에서 최상의 구성요소를 결합한 기타 업체의 새로운 제품뿐 아니라 보안 제품의 IBM SecureWay 계열로 제공됩니다. 이외에도, 구현 서비스는 선택된 FirstSecure 구성요소에서도 사용할 수 있습니다. FirstSecure 구축 블록은 다음과 같습니다.

- SecureWay Policy Director
- SecureWay Boundary Server
- Intrusion Immunity
- IBM SecureWay Trust Authority에서 제공되는 공용 키 하부구조
- IBM SecureWay Toolbox

FirstSecure는 독립적으로 설치될 수 있는 제품의 컬렉션이므로 보안 환경 쪽으로 이끌어 나갈 수 있습니다. 하나의 영역에서 시작하여 개선점을 테스트한 후 계속 보안쪽으로 이동해 나가면 됩니다. 이는 복잡성과 비용을 줄이고 웹 응용 프로그램 및 자원의 전개 속도를 가속화합니다.

FirstSecure가 필요한 이유는?

사용자 데이터와 자원은 e-business에서 중요합니다. FirstSecure의 제품은 함께 다음을 제공합니다.

권한 부여

모든 사용자는 규칙을 따라야 합니다. 권한 부여는 시스템, 데이터, 응용 프로그램 및 네트워크에 대해 승인된 사용자 액세스만 허용합니다.

책임 언제 누가 무엇을 했는지 알 수 있습니다. 책임을 통해 누가 조치를 수행했는지와 지정된 시간 간격 중에 어떤 조치가 발생했는지를 판별할 수 있습니다.

보장 시스템에서 보안 약속을 이행하는지 보장할 수 있습니다. 이 보호를 통해 요구한 보안 보호 레벨이 강제 수행되는지를 보여주고 그 유효성을 검증할 수 있습니다.

가용성 시스템은 필요할 때 사용할 수 있습니다. 이 보호는 직원, 공급업자, 파트너 및 고객이 시스템, 데이터, 네트워크 및 응용 프로그램을 사용할 수 있도록 유지하는데 도움을 줍니다.

관리 규칙을 정의할 수 있습니다. 이 보호는 정책 정보를 정의, 유지보수, 모니터 및 수정할 수 있게 합니다.

기업 전반에 걸친 정책을 기반으로 이런 보호를 구현하여 엔터프라이즈의 전체 네트워크, 시스템 및 응용 프로그램 세트에서 보호망을 제공합니다. 그 망의 제품 간에 있는 취약한 링크는 나머지 하부구조를 쓸모없게 할 수 있습니다.

이 책은 각 SecureWay 구축 블록 제품을 제공된 보호 목록에 연결합니다.

FirstSecure 구축 블록은 무엇입니까?

FirstSecure에는 모든 제품의 그룹으로 또는 별도의 관련 제품으로 얻을 수 있는 구성요소 제품이 들어 있습니다. 이런 제품에는 하나 이상의 구성요소 제품이 있을 수 있습니다. 아무 제품에서 시작하여 보안 솔루션을 완료할 수 있습니다.

Policy Director

Policy Director는 보안 계획의 중심입니다. Policy Director는 지리적으로 분산되어 있는 인트라넷과 엑스트라넷에서 웹 자원을 완벽하게 보안하기 위해 권한을 부여하고 관리합니다. Policy Director는 인증, 권한 부여, 데이터 보안 및 자원 관리를 제공합니다. 표준 인터넷 기반 응용 프로그램과 함께 Policy Director를 사용하여 안전하고 잘 관리된 인트라넷을 구축하십시오. Policy Director에는 다음이 포함됩니다.

- 보안 서비스
- 관리 콘솔
- 관리 서버
- 보안 서버(NetSEAL 및 WebSEAL)
- NetSEAT 클라이언트
- 디렉토리 서비스 브로커
- 권한 부여 서버(타사 응용 프로그램 지원)

Policy Director는 Windows NT, AIX 및 Solaris에서 실행합니다.

Policy Director의 완전한 설명에 대해 35 페이지의 『제5장 네트워크에서의 Policy Director 계획』을 참조하십시오.

SecureWay Boundary Server

SecureWay Boundary Server 제품은 웹 기반 e-business 응용 프로그램에 대해 보장, 관리 및 책임을 제공합니다. 보안 경계는 엔지니어링 및 인적 자원과 같은 부서 간, 본사 네트워크와 지사 간, 사내 네트워크와 인터넷 간, 회사의 웹 응용 프로그램과 고객 간, 사내 네트워크와 영업 파트너 간 등 모든 곳에서 필요합니다. 적절한 경계 보안에서는 네트워크를 액세스할 수 있는 사람과 네트워크에서 입력되거나 출력되는 정보를 제어할 수 있습니다.

이 섹션은 SecureWay Boundary Server의 구축 블록을 설명합니다. 계획 및 통합 고려사항에 대해서는 65 페이지의 『제12장 SecureWay Boundary Server 요구사항 및 설치 고려사항』을 참조하십시오.

IBM SecureWay Firewall

IBM Firewall이라고도 하는 IBM SecureWay Firewall은 인터넷과의 모든 통신을 제어하여 보다 안전한 e-business를 가능하게 합니다. IBM Firewall은 필터링, 프록시 및 회선 레벨 게이트웨이와 같은 3가지 중요한 Firewall 기능을 제공하여 높은 수준의 보안과 융통성을 제공합니다.

ACE/Server

Security Dynamic의 ACE/Server에는 SecurID 토큰(사용자 라이센스 2개와 토큰 2개)이 들어 있습니다. ACE/Server는 관리자 로그온과 *VPN(virtual private network)* 연결을 IBM SecureWay Firewall에 추가합니다.

IBM SecureWay 릴리스 2용 MIMEsweeper

Content Technology의 MIMEsweeper에는 인터넷 보안의 구성요소가 들어 있습니다. MAILsweeper는 이메일을 확인하여 기밀 정보가 e-business에서 유출되지 않고 허용되지 않은 이메일이 들어오지 않도록 합니다.

WEBsweeper는 원하지 않는 웹 자료가 비지니스에 들어오지 못하도록 유지합니다. 이는 허용된 Java 애플릿, 실행 코드 또는 웹 사이트에서만 데이터를 스캔하고 승인합니다.

SurfinGate

Finjan Software Ltd.의 SurfinGate는 e-business의 모빌 코드 보안 솔루션입니다. 모빌 코드는 이제 자동으로 인트라넷 외부에서 e-business 네트워크로 정기적으로 들어오므로 Firewall 이상의 보호가 필요합니다. SurfinGate는 Java, ActiveX 및 JavaScript 코드의 침입으로부터 네트워크를 보호합니다. 이는 중요한 자원에 대한 공격이 네트워크에 들어오기 전에 이를 식별합니다. 이는 의심이 가는 데이터를 받아들이기 전에 사용자가 조사할 수 있도록 격리합니다.

Intrusion Immunity

Intrusion Immunity는 엔터프라이즈 감지 및 보호 제품의 형식으로 보장을 제공합니다. Intrusion Immunity 요구사항에 대해 73 페이지의 『제13장 Intrusion

Immunity 요구사항 및 설치 고려사항』을 참조하십시오. Intrusion Immunity에는 Tivoli Cross-Site for Security와 Norton AntiVirus가 있습니다.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security는 공격하기 쉬운 시스템에 침입 감지 기능을 제공합니다. Tivoli Cross-Site for Security를 사용하여 다음을 수행할 수 있습니다.

- 네트워크에 Cross-Site for Security 에이전트를 설치하여 의심가는 사건을 Cross-Site for Security 관리 서버에 보고합니다.
- 사전 정의된 사용자 설치 보고서에서 침입 데이터를 봅니다.
- 실시간에 권한 부여받지 않았거나 의심가는 활동을 감지하고 로그합니다.
- 거짓 알람의 수를 줄일 수 있도록 보안 에이전트를 조정합니다.

Norton AntiVirus

Symantec Corporation의 제품인 Norton AntiVirus는 세계적인 바이러스 방지 소프트웨어 제품 중 하나입니다. Norton AntiVirus는 백그라운드에서 계속 실행하여 이메일 첨부, ActiveX 제어, Java 애플릿, 인터넷 다운로드, 디스켓, 소프트웨어 CD 또는 네트워크를 통해 전송된 파일과 함께 들어올 수 있는 바이러스로부터 컴퓨터를 안전하게 지킬 수 있습니다. Norton AntiVirus를 가지고 감염된 파일을 격리할 수 있습니다. Norton AntiVirus는 갱신사항과 새로 발견한 바이러스를 자동으로 알릴 수 있도록 구성할 수 있습니다.

공용 키 하부구조

IBM FirstSecure는 IBM SecureWay Trust Authority에서 암호화와 상호 조작 가능성에 대한 공용 키 하부구조(PKI) 표준을 지원합니다.

SecureWay Trust Authority는 디지털 인증서의 발급, 갱신 및 취소를 지원하는 보안 솔루션입니다. 이런 인증서는 사용자를 인증하는 수단을 제공하고 신뢰할 수 있는 통신을 보장하면서 광범위한 인터넷 응용 프로그램에 사용할 수 있습니다. Trust Authority는 *IETF(Internet Engineering Task Force)*의 *PKI(Public Key Infrastructure)* 작업 그룹 스펙을 기반으로 합니다. 여기에는 다음이 포함됩니다.

- IBM AIX와 Microsoft Windows NT에 대한 지원
- 등록 기관(RA)
- 인증 기관(CA)
- 인증서를 요청하고 발급된 인증서를 관리하는 사용자 인터페이스
- 통합된 *IBM SecureWay Directory*
- *감사* 서브 시스템
- SecureWay 4758 암호 보조 프로세서 지원
- *스마트 카드* 지원

이 하부구조는 등록과 *초기* 인증서, 키 쌍 갱신, 인증서 갱신, 인증서 및 인증서 취소 목록 게시 및 인증서 취소를 포함한 완전한 인증서 수명을 지원합니다. 자세한 내용은 81 페이지의 『제14장 공용 키 하부구조 요구사항 및 설치 고려사항』를 참조하십시오.

Toolbox

FirstSecure Toolbox는 FirstSecure의 주요 구성요소의 일부이거나 이와 상호 조작 가능한 보안 및 보안 관련 툴킷의 세트입니다. 툴킷은 다음에 도움을 줍니다.

- FirstSecure와 응용 프로그램을 통합합니다.
- FirstSecure를 사용하여 솔루션과 응용 프로그램을 사용자 정의합니다.
- FirstSecure를 사용하는 ISV와 OEM 응용 프로그램을 작성합니다.

FirstSecure Toolbox 툴킷 API는 다음과 같은 보안 기능을 지원합니다.

- 권한 부여 서비스
- 인증서 및 관리 서비스
- 디렉토리 서비스
- SSL(Secure Sockets Layer) 프로토콜 서비스
- KeyWorks 암호 및 신뢰 관리 서비스
  - IBM Key Recovery Service Provider 1.1.3.0 API. IBM Key Recovery Service Provider를 통해 암호화된 정보를 복구할 수 있습니다.

– IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0은 권한 부여된 요청으로 키를 사용할 수 없거나 유실 또는 훼손된 경우 암호화된 정보를 복구할 수 있는 응용 프로그램입니다.

이런 두 툴킷은 응용 프로그램이 중요한 보안 서비스뿐만 아니아 보안 제공자가 툴킷에 플러그인하기 위해 사용할 수 있는 표준 인터페이스를 호출할 때 사용하는 표준 인터페이스를 제공합니다. 표준 인터페이스는 CDSA(Common Data Security Architecture)를 기반으로 합니다. 이런 툴킷은 Windows NT, Solaris 및 AIX에서 사용할 수 있습니다.

구현 서비스

FirstSecure 구현 서비스는 e-business에서 FirstSecure를 빠르고 효율적으로 시작하고 수행할 있게 도와줍니다. 이러한 별도로 가격이 정해져 있는 서비스들은 IBM이 제공하며 경험있는 컨설턴트 팀에서 수행합니다. FirstSecure 구현 서비스에는 FirstSecure 구현 워크샵과 제품 레벨의 QuickStart 설치 서비스가 있습니다. IBM은 또한 사용자의 환경에 맞게 사용자 정의된 FirstSecure 시스템 통합 서비스를 제공할 수 있습니다.

옵션 정보 및 가격에 대해서는 IBM 담당자에게 문의하십시오.

제2장 릴리스 2의 새로운 기능

릴리스 2는 IBM SecureWay FirstSecure 제품의 계획과 설치 과정을 단순화시킵니다. 각각의 제품은 더욱 통합되고 제품은 추가되었으며 관리 및 제어는 중앙 집중화되었습니다.

Policy Director

Policy Director에는 다음과 같은 개선사항이 있습니다.

- 사용자 및 그룹 인증사항 정보의 저장영역용 IBM SecureWay Directory에 대한 지원.
- Open Group의 권한 부여 API 스펙에 대한 최신 갱신.
- Policy Director 관리 콘솔을 사용하여 IBM Firewall 프록시 사용자 인증사항을 정의하고 편집할 수 있는 기능.
- 외부 인증 서비스의 사용을 지원하는 Policy Director CAS(Credentials Acquisition Service).
- 새 Policy Director CAS를 사용한 클라이언트측 인증서 기반 인증 지원.
- WebSEAL과 Policy Director CAS 간에 IDL(Interface Definition Language)를 사용하여 자신의 사용자 정의된 인증사항 획득 서비스를 작성할 수 있는 기능. Policy Director는 또한 시동, 서버 등록 및 신호 처리와 같은 Policy Director CAS 서버 기능을 처리하는 일반 서버 프레임워크를 제공합니다.
- GSS(Generic Security Service) 터널링 외에 SSL(Secure Sockets Layer) 터널링 메커니즘을 사용할 수 있는 선택 항목.
- 로그인 및 암호 정책을 관리하기 위해 Policy Director 관리 콘솔이나 명령 행 인터페이스 사용.
- 단일 사인온 사용자, 그룹 및 자원(목표)를 관리하기 위해 Policy Director 관리 콘솔이나 명령 행 인터페이스 사용.
- 웹 기반 단일 사인온 목표 암호 관리 툴.
- 통합된 설치 프로세스.

SecureWay Boundary Server

SecureWay Boundary Server에는 다음과 같은 개선사항이 있습니다.

- SecureWay Boundary Server와 Policy Director의 일부 기능을 함께 연결하는 구성 GUI.
- SecureWay Boundary Server와 Policy Director의 일부 기능을 함께 연결하는 새 구성 TaskGuide.

AIX 및 NT용 IBM SecureWay Firewall의 새로운 기능

IBM Firewall라고도 하는 IBM SecureWay Firewall에는 다음과 같은 개선사항이 있습니다.

보안 메일 프록시 개선사항

IBM Firewall 보안 메일 프록시는 다음과 같은 새 기능을 포함하도록 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 Anti-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 개선사항

Socks 프로토콜 버전 5는 사용자 이름 암호 인증(UNPW), 도전/응답 인증(CRAM) 및 인증 플러그인을 포함하도록 업그레이드되었습니다.

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

HTTP 프록시

IBM SecureWay Firewall은 IBM WTE(Web Traffic Express) 제품을 기반으로 완전하게 기능하는 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 HTTP 프록시를 구현하기 위해 클라이언트 환경을 변경하지 않고 인터넷에서 유용한 정보를 액세스할 수 있습니다.

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 데이터를 닮을 수 있도록 기초를 이루는 PPP 데이터를 변환하는 네트워크 드라이버입니다.

AIX용 IBM SecureWay Firewall 개선사항

AIX용 IBM SecureWay Firewall은 다양한 확장사항을 제공합니다.

향상된 IPSec 지원

향상된 IPSec 지원에는 새 헤더에 대한 지원이 포함됩니다. 이는 또한 여러 IBM 서버와 라우터뿐만 아니라 새 헤더를 지원하는 여러 IBM 이외의 VPN 제품과의 상호 조작 가능성을 지원합니다.

다중프로세서(MP) 지원

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

필터 개선사항

구성과의 더 나은 성능과 더 나은 융통성. 서로 다른 유형의 필터 규칙을 찾을 위치를 선택하여 IBM SecureWay Firewall의 성능을 조정할 수 있습니다. 빈도 표시기는 연결을 사용하는 횟수를 제공합니다.

네트워크 주소 변환

다대일 주소 맵핑 지원. 이런 맵핑은 여러 개의 등록되지 않은 내부 또는 개인 주소에서 포트 번호를 사용하여 고유한 맵핑을 작성하는 등록된 적법한 주소로 이루어집니다.

설정 마법사

마법사는 IBM Firewall의 초기 구성에 도움을 줍니다. 이 설정 마법사를 사용하면 IBM Firewall에 대해 광범위한 지식이 없는 사용자가 기본 구성을 설치 후 빠르게 시작하고 수행할 수 있습니다.

네트워크 보안 감사기

NSA(Network Security Auditor)는 보안 틈이나 구성 오류에 대해 네트워크 서버와 IBM Firewall을 확인합니다. 이는 더 빠르고 더 견고합니다.

IBM SecureWay 릴리스 2용 MIMEsweeper의 새 기능

MAILsweeper 개선사항에는 다음이 포함됩니다.

- 괴롭힘이나 비방하는 메일을 차단하기 위한 주요 단어를 스캔하고 회사에서 중요한 데이터가 빠져나가지 않도록 보호합니다.
- 들어오는 불필요한 이메일을 차단합니다.
- 지정된 유형의 파일을 송신하거나 수신하지 못하도록 개인이나 그룹을 차단합니다.
- 네트워크 경합을 피하기 위해 크기별로 파일을 차단하거나 지연시킵니다.

WEBsweeper 개선사항에는 다음이 포함됩니다.

- 직원을 작업에 관련없는 지정된 사이트로부터 차단합니다.
- HTML이나 이메일 주소를 통해 문서를 추출하고 쿠키를 통해 사이트 정보를 추출하는 공격으로부터 보호하는데 도움을 줍니다

SurfinGate의 새 기능

SurfinGate에는 다음과 같은 개선사항이 있습니다.

- JavaScript 내용 검사
- 업무별 중요 성능 모니터링
- 증가된 정책 관리
- FTP(File Transfer Protocol)와 HTTPS 프로토콜 지원
- Firewall HTTP 프록시와의 플러그인 통합

- 특정 실행 파일이 사용자 컴퓨터로 다운로드되지 않도록 차단하는 기능

Intrusion Immunity

Intrusion Immunity에는 이제 Tivoli Cross-Site for Security가 들어 있습니다.

Tivoli Cross-Site for Security의 새 기능

Tivoli Cross-Site for Security는 침입 감지 기능을 제공합니다. 이를 통해 사용자는 e-business의 통합성에 대한 네트워크 공격을 모니터합니다.

Norton AntiVirus Solution Suite의 새 기능

Norton AntiVirus Solution Suite, 릴리스 3.0.4에는 다음과 같은 갱신된 버전이 있습니다.

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

공용 키 하부구조

공용 키 하부구조 구성요소에는 이제 Trust Authority이 들어 있습니다. Trust Authority에는 다음을 포함합니다.

- Windows NT에서의 간단한 설치를 안내해 주는 설치 마법사.
- 4758 암호 카드의 사전 설정된 구성. 이 정보를 변경할 수 있습니다.
- 배경 구성 프로그램이 시작하기 전에 데이터의 유효성을 확인하는 구성 마법사.
- 오류 메시지 및 보고.
- 설정 마법사, 등록 기관 데스크탑 및 엔드-엔티티 클라이언트 응용 프로그램에 대한 내용별 도움말을 포함하는 온라인 문서.

IBM SecureWay Toolbox

Toolbox에는 다음과 같은 개선사항이 있습니다.

- Policy Director API 및 문서.
- 디렉토리 서비스 API.
- 공용 키 하부구조(PKIX) API 및 문서.
- IBM Key Recovery Server 1.1.3.0은 이제 Toolbox에 포함되어 있습니다. 이 제품은 영어로만 사용할 수 있습니다.

제2부 보안 e-business 네트워크 계획

제2부에서는 보안 e-business 네트워크에 대한 계획을 설명합니다.

다음 장에서는 일반적인 인터넷 트래픽과 보안 관련 사항에 대해 설명한 후 FirstSecure 제품이 e-business 네트워크에서 어떻게 작동하는지를 알려줍니다.

이 섹션은 다음과 같은 장으로 구성됩니다.

- 19 페이지의 『제3장 e-business 네트워크 개요』는 일반적인 e-business 네트워크와 네트워크상의 사용자, 자원 및 상호 작용의 종류를 설명합니다. 네트워크에는 더 많거나 더 적은 수의 기능이 있을 수 있지만 같은 보안 문제를 가지며 같은 보안 보호가 필요합니다.
- 31 페이지의 『제4장 e-business 네트워크에서의 FirstSecure 계획』은 FirstSecure 제품을 네트워크에 연결합니다.
- 35 페이지의 『제5장 네트워크에서의 Policy Director 계획』
- 39 페이지의 『제6장 네트워크에서의 SecureWay Boundary Server 계획』
- 45 페이지의 『제7장 네트워크에서의 Intrusion Immunity 계획』
- 53 페이지의 『제8장 네트워크에서의 공용 키 하부구조 계획』

제3장 e-business 네트워크 개요

e-business 네트워크는 데이터와 데이터베이스, 사용자, 고객, 공급업자, 프로그래머, 하드웨어, 회사 정보 등의 자원으로 구성됩니다. 이런 영역 중 일부를 살펴보고 어디에서 보안이 필요한지 알아봅시다.

인터넷은 복잡합니다. 데이터는 전송할 때마다 변하는 정의되지 않은 경로를 통해 서버 간에 및 사용자 간에 전달됩니다.

인터넷을 통한 비지니스 데이터 전송은 다른 모든 인터넷 트래픽과 섞입니다. 그 경로를 따라 비지니스에 중요한 데이터는 다른 곳에 있는 서버를 통과했을지도 모릅니다. 어떤 인터넷 사용자는 자원, 직원 및 데이터를 액세스하려고 시도했을지도 모릅니다. 불행히도, 교육, 비지니스 및 오락을 위한 적법한 트래픽 외에도 무해하거나 고의적인 유해한 트래픽을 운반할 수도 있습니다. 20 페이지의 그림1은 모든 사용자의 트래픽으로 채워진 인터넷을 통과하는 해당 사용자의 트래픽의 개요입니다.

FirstSecure는 다른 모든 트래픽에서 사용자의 전송을 분리하고 보안할 수 있게 도와줍니다.

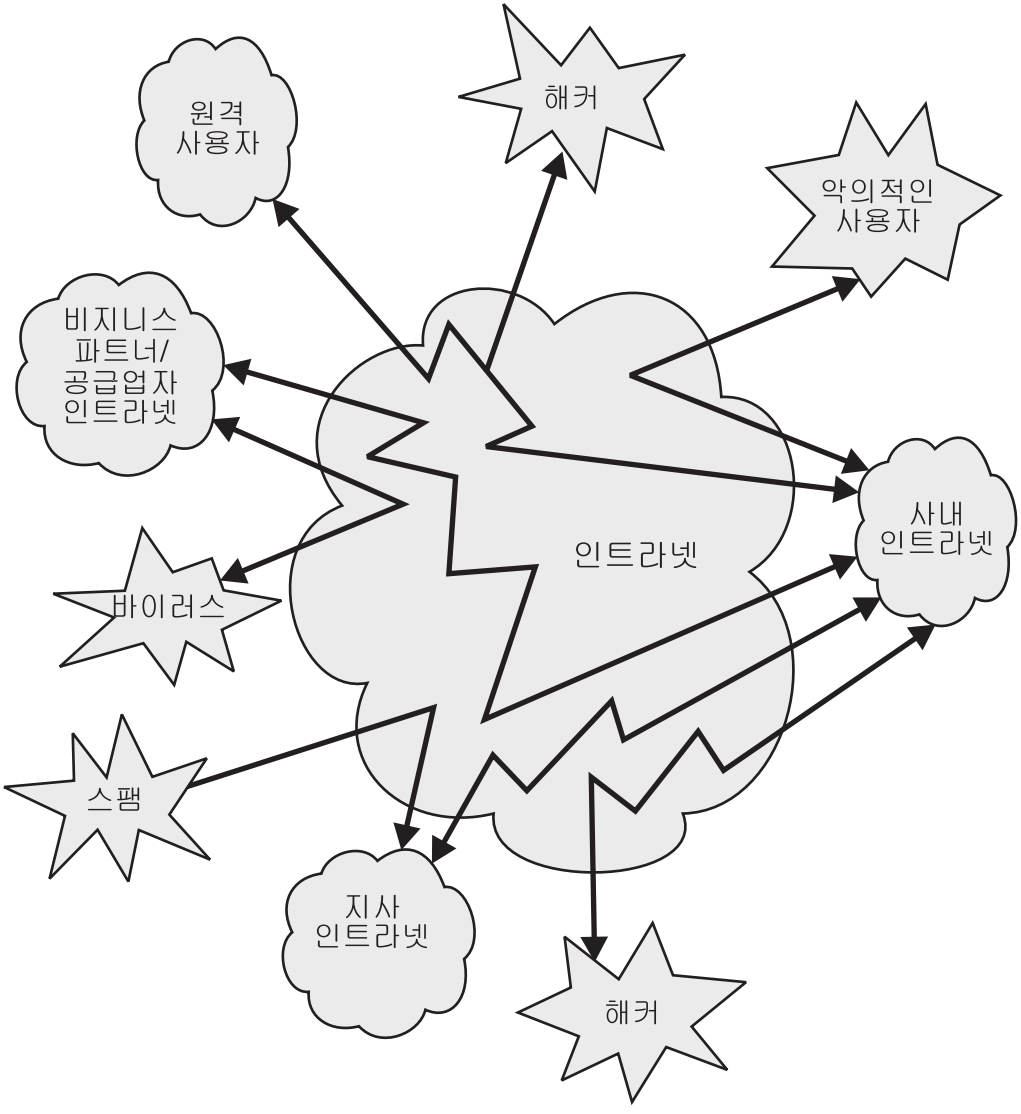


그림 1. 관련 없는 활동으로 바쁜 인터넷 개요

이런 인터넷 보기에서 작업하고 싶지 않을 것입니다. FirstSecure로 보안된 인터넷인 21 페이지의 그림2의 뷰를 원할 것입니다.

FirstSecure에 의해 보호된 이상적인 인터넷

e-business 트래픽의 대부분은 인터넷을 통과합니다. 그러나, 인터넷을 홈 컴퓨터가 있는 거의 모든 사람들에게 노출되어 있는 거대한 데이터 컬렉션으로 보고 싶지 않을 것입니다. 그림2는 원하는 인터넷을 보여줍니다.

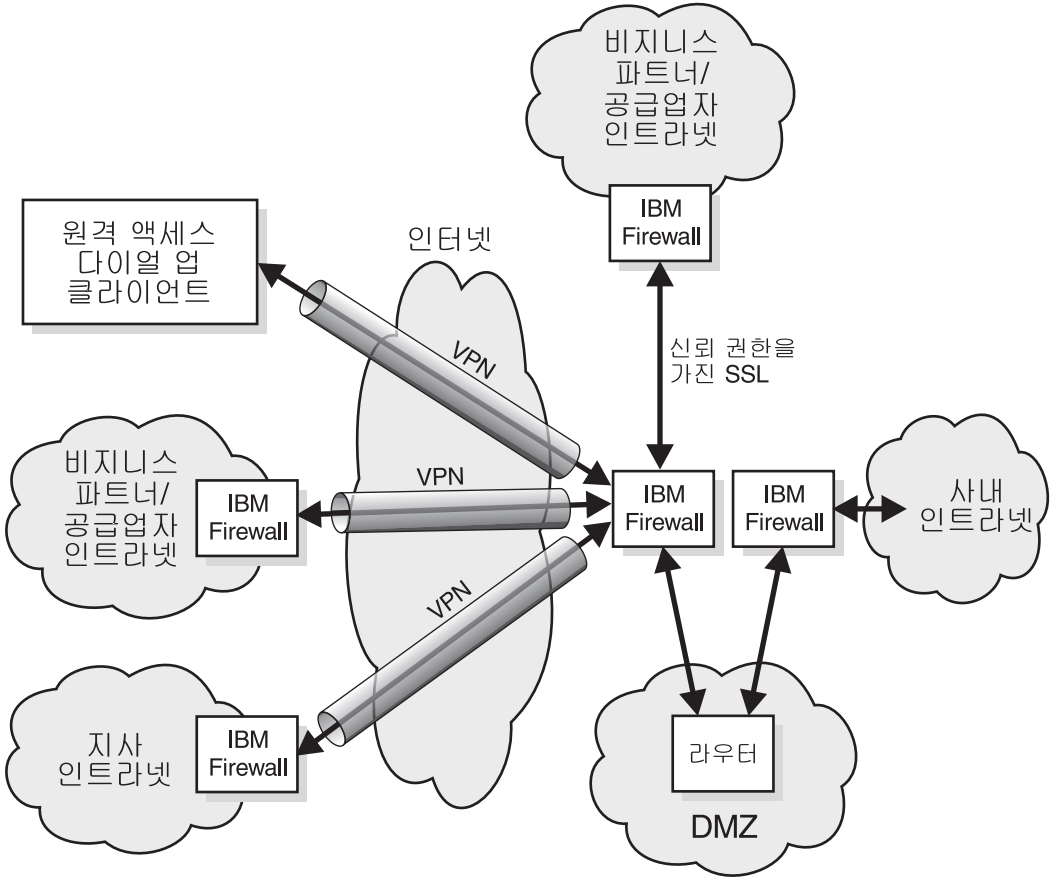


그림 2. 원하는 인터넷

인터넷을 통해 좋은 정보를 많이 얻을 수 있는 반면 비지니스에서 보호하고 싶은 응용 프로그램, 데이터 및 액세스가 있습니다. 사용자는 다음과 같은 상황을 보장하고 싶을 것입니다.

- 직원은 할당된 작업에서 벗어나지 않습니다.

- 직원은 부적절한 이메일로부터 보호됩니다.
- 중요한 비지니스 정보는 비지니스내에서만 사용됩니다.

VPN(virtual private network)

VPN(virtual private network)는 인터넷을 통해 다른 사용자가 액세스할 수 없는 개인 연결 개념입니다. 그림3은 일반적인 VPN을 보여줍니다. 각 끝에 있는 사용자에게까지 연결되며 이는 원하지 않는 사용자나 응용 프로그램의 침입으로부터 안전합니다. IBM SecureWay Firewall과 같은 FirstSecure 제품은 VPN을 설정하고 지원하는데 도움을 줍니다.

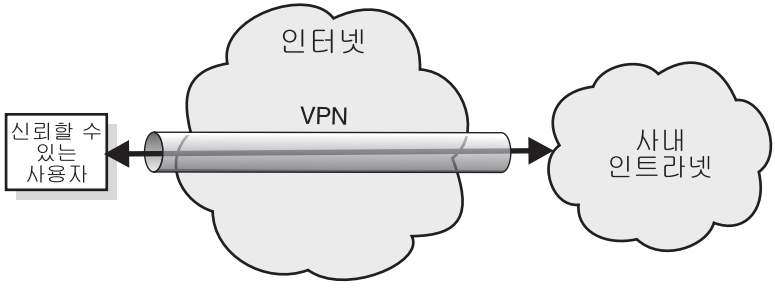


그림 3. 일반적인 VPN(virtual private network)

DMZ(demilitarized zon)

*DMZ(demilitarized zon)*는 외부 사용자가 액세스할 수 있는 자원 본체입니다. IBM Firewall, MIMEsweeper 및 기타 FirstSecure 제품을 사용하여 원하는 사용자만 DMZ를 액세스하고 지정된 자원만 액세스할 수 있도록 만들 수 있습니다. DMZ에서 주고 받는 트래픽은 그 적합성 여부를 판별하기 위해 모니터되어야 합니다.

회사의 카탈로그는 잠재적 고객이 찾아볼 수 있도록 DMZ에 있을 수 있습니다. 또는 회사를 소개하는 참조용 팜플렛이 있을 수 있습니다. FirstSecure 구성요소를 사용하면 신뢰할 수 있는 사용자만 DMZ 뒤에 있는 정보를 액세스할 수 있습니다.

23 페이지의 그림4는 일반적인 DMZ를 보여줍니다.

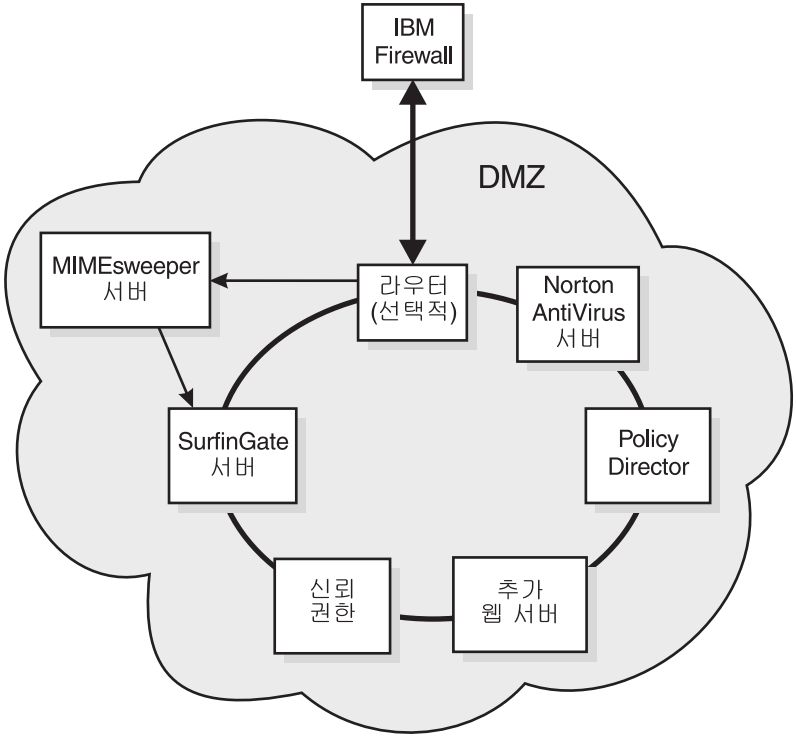


그림 4. 시스템 자원이 있는 일반적인 DMZ

보안 응용 프로그램을 개발하면서 이런 응용 프로그램에 공용 액세스 권한을 부여하기 전에 DMZ를 인트라넷 테스트 기반으로 사용할 수 있습니다.

이제 인터넷과 인트라넷을 사용하는 정보의 종류에 대해 알아봅시다.

일반적인 사내 인트라넷

사내 인트라넷은 사내에서 서로 통신하는 곳입니다. 여기에는 인터넷에서 공유하지 않는 정보와 자원이 있습니다. 직원은 데이터를 공유하고 서로 이메일을 주고받으며 데이터베이스, 프린터 및 스캐너와 같은 회사 자원을 액세스합니다. 24 페이지의 그림5는 일반적인 사내 인트라넷을 보여줍니다.

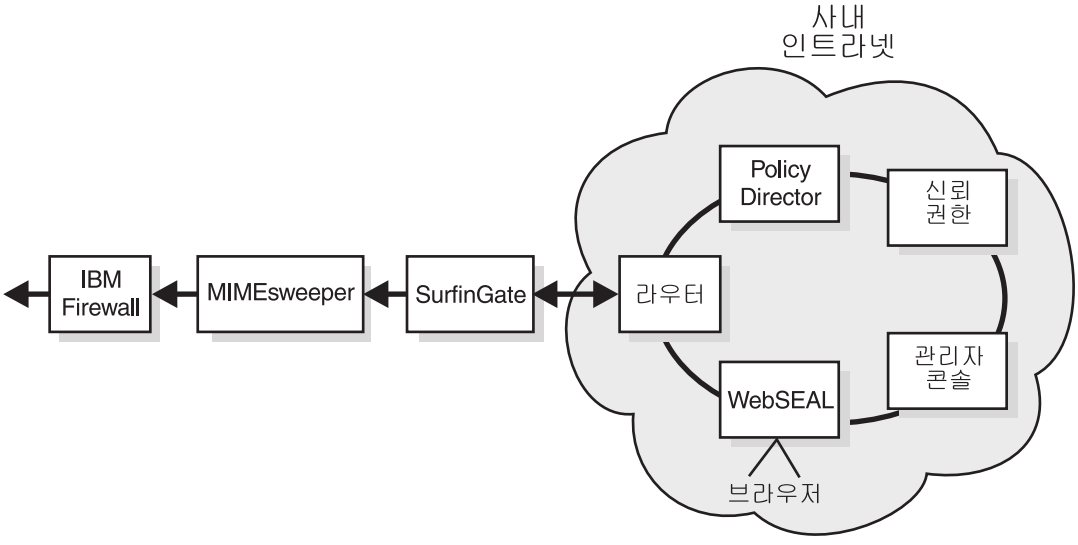


그림 5. 일반적인 사내 인트라넷 개요

회사의 기밀 정보는 사내에서만 사용되도록 해야 하며 그 데이터에 대한 액세스 권한을 받은 사람들만 액세스할 수 있도록 해야 합니다. 그러나, 고객이 사용하고 액세스할 수 있는 데이터도 있습니다. 예를 들어, 은행의 예금자는 잔액을 확인할 수 있지만 직원 레코드를 액세스하지는 못합니다. IBM Firewall은 개인 정보를 개인용으로 유지합니다.

IBM FirstSecure 제품은 인트라넷 보안을 유지할 수 있게 도와 줍니다. Policy Director를 통해 액세스 규칙을 설정할 수 있습니다. IBM SecureWay Trust Authority는 사용자가 주장하는 사용자와 동일한지를 확인합니다. Tivoli Cross-Site for Security를 통해 사용자는 권한을 부여 받지 않은 상태에서 인트라넷 자원을 액세스하려는 시도가 있었는지를 알 수 있습니다.

일반적인 지사 인트라넷

지사에 근무하는 원격 직원은 사내의 직원과 같은 데이터와 자원을 액세스해야 합니다. 그러나, 정보 송수신에 사용되는 전화선은 느리고 고의에 의한 간섭으로부터 보호 받지 못합니다. 인터넷은 트랜잭션을 더 안전하게 보호하거나 비용 절감의 수단으로 사용할 수 있습니다. 그림6은 인터넷을 통해 본사와 통신하는 일반적인 지사를 보여줍니다.

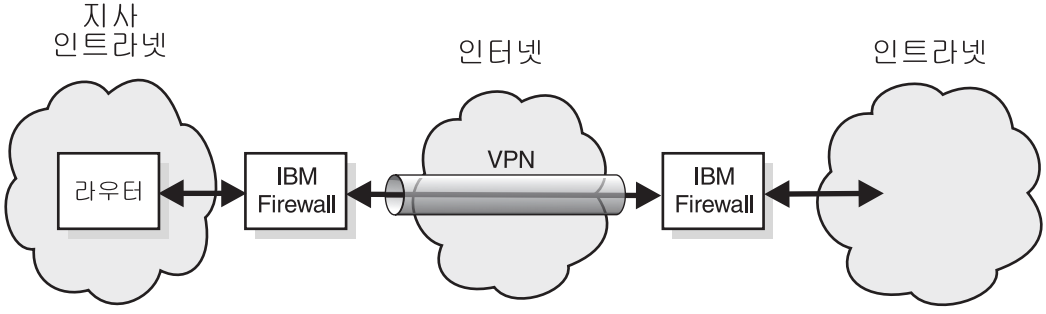


그림 6. VPN(virtual private network)를 통해 본사와 연결된 지사

사용자는 트랜잭션과 데이터가 엔터프라이즈에서 마치 한 장소에 있는 것처럼 안전하길 원합니다. *VPN(virtual private network)*는 인터넷을 통과하는 터널입니다. 인터넷을 마치 사설 인트라넷 네트워크처럼 사용합니다.

일반적인 원격 액세스 직원

일부 직원은 때때로 또는 영구적으로 본사에서 떨어진 장소에서 근무할 수 있습니다. 직원은 다이얼 업이나 전용 연결을 사용하여 인터넷을 통해 네트워크를 액세스할 수 있습니다.

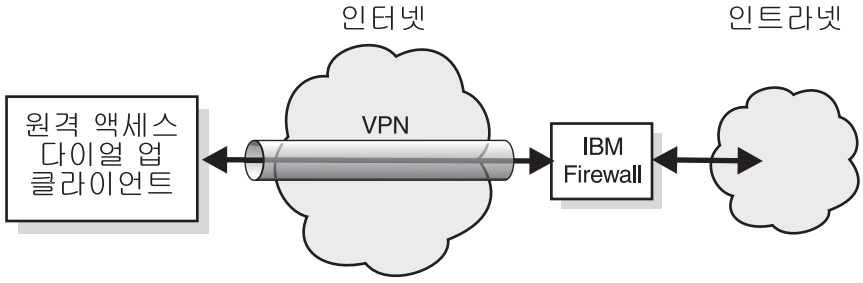


그림 7. VPN(virtual private network)를 통해 본사에 연결된 원격 다이얼 업 클라이언트

IBM Firewall은 이 직원의 전송을 보호합니다.

일반적인 비지니스 파트너 또는 공급업자 인트라넷

비지니스는 비지니스 파트너와 공급업자가 일부 데이터를 직접 액세스할 수 있을 때 더 효율적입니다. 한 공급업자는 재고 수준을 확인하고 지정된 레벨의 새 제고를 보낼 수 있는 권한이 있을 수도 있습니다. 또 다른 비지니스 파트너는 선택된 레코드를 액세스할 수 있을 수도 있습니다. 경리 회사는 기타 세금 레코드에 대한 액세스 권한은 필요하지만 비지니스 파트너의 레코드에 대한 액세스 권한은 필요하지 않습니다. 27 페이지의 그림8 및 27 페이지의 그림9는 일반적인 공급업자나 비지니스 파트너를 보여줍니다. 사용자는 비지니스 트랜잭션이 마치 개인 연결에서 이동하는 것처럼 인터넷에서 이동하길 원합니다.

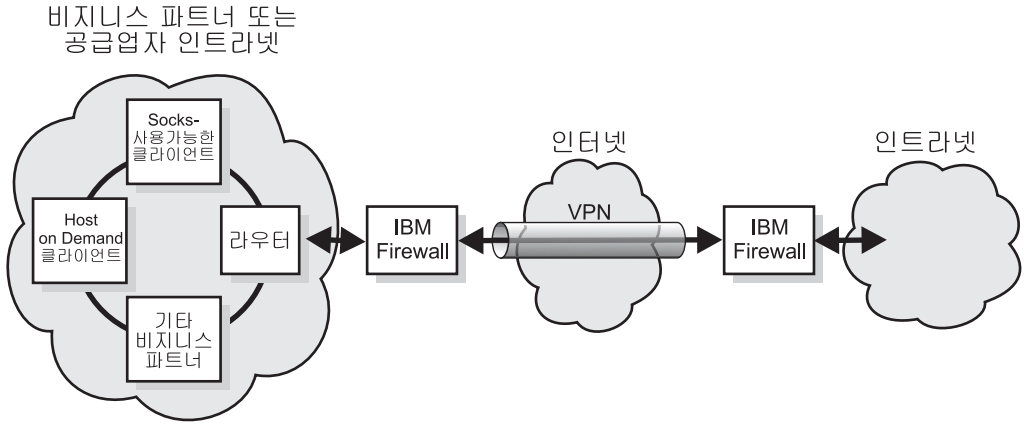


그림 8. VPN(virtual private network)를 사용하는 일반적인 비지니스 파트너나 공급업자 인트라넷

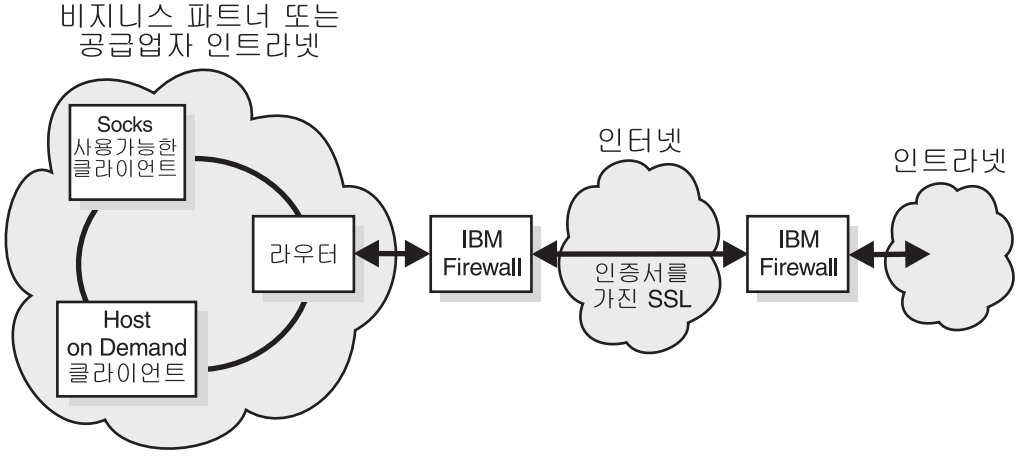


그림 9. SSL(Secure Sockets Layer) 전송 프로토콜을 사용하는 일반적인 비지니스 파트너나 공급업자 인트라넷

이 비지니스 파트너는 전송이 종단간 암호화되므로 VPN을 사용하는 대신 SSL을 사용합니다.(사용자는 추가 보안 계층에서도 VPN을 사용할 수 있습니다.)

이런 사용자를 서로 보호해 주고, 고의적인 간섭과 침입자들로부터 보호해 줘야 합니다. 이런 사용자의 데이터 전송을 권한을 부여 받지 않은 청취자와 전송자로부터 보호해야 합니다. 또한, 이런 사용자가 액세스할 수 있도록 허용한 데이터만 액세스하도록 해야 합니다. 그리고 이런 사용자는 예상한 사용자이어야 합니다.

데이터 및 데이터베이스

데이터는 비지니스에서 소유하는 가장 귀중한 자원입니다. 일부 e-business 데이터는 모든 인터넷 사용자가 사용할 수 있도록 설계되었습니다. 예를 들어, 하드웨어 판매자는 온라인 쇼핑에 사용하도록 그 재고와 가격 목록을 제공할 수도 있습니다. 옷감 소매업자는 온라인 쇼핑을 위해 스타일, 색상 및 크기의 온라인 카탈로그를 제공할 수 있습니다.

데이터에 대한 액세스를 허용하기 전에 요청자가 누구인지를 알아야 하고 그 데이터를 요구하는 이유를 알아야 합니다. Trust Authority를 사용하여 신뢰할 수 있는 사용자에게 인증서를 발급하십시오.

보호해야 하는 기타 영역

이 책은 기타 보안 영역에 대한 대책을 다루지는 않습니다. 다음에 대해서도 계획해야 합니다.

- 사이트 보안, 액세스 및 출구 및 구분
- 랩톱 컴퓨터, PC 및 워크스테이션 및 기타 컨테이너의 물리적 보안
- 개인 보안 백그라운드 확인
- 책임, 계약 등에 대한 합법적인 거부
- 키 관리, 정보 제어 및 보안 인식 및 교육과 같은 조작적 연습

운영 체제

대부분의 운영 체제는 고가용성과 풍부한 기능 세트를 위해 구성됩니다. 효과적인 보안 접근 방법은 주어진 작업을 수행하는데 있어서 필요한 최소한의 기능만 사용하는 것입니다. 침입자가 액세스하지 못하도록 모든 운영 체제 기능을 설치 제거하거나 사용할 수 없게 만드는 것에 대해 고려해 봐야 합니다.

일반 사용자

인터넷에는 일부는 적절하고 일부는 적절하지 못한 여러 유형의 사용자가 있습니다. e-business는 온라인으로 탐색하고 구매하는 고객인 사용자를 원합니다. e-business는 또한 비지니스 파트너가 특정 데이터를 액세스하여 재고를 확인하고

제조 결정을 하거나 비지니스내에서의 계획과 활동에 의견을 제시하기를 원합니다. e-business는 또한 직원이 할당된 작업을 수행하기 위해 필요한 데이터를 액세스할 수 있기를 원합니다.

인터넷에는 해커, 스패머, 바이러스 배포자, 중요한 데이터를 액세스하려는 사용자 등 e-business에서 원하지 않는 사용자도 있습니다. 이런 사용자는 사용자의 e-business내에 있을 수도 있습니다.

자원의 액세스를 허용하기 전에 요청하는 사용자가 누구인지, 그 사용자가 데이터와 응용 프로그램에 대해 어떤 유형의 액세스 권한이 있는지 그리고 어떤 사용자 액세스 레코드를 보관해야 하는지를 알아야 합니다.

응용 프로그램 및 응용 프로그램 작성

응용 프로그램은 보안을 포함하도록 설계될 수 있습니다. 전송될 데이터의 암호화, 액세스를 요구하는 사용자의 인증, 사용자 및 트랜잭션의 감사 로그를 활용할 수 있습니다.

Toolbox API를 통해 응용 프로그램에 보안을 추가할 수 있습니다.

하드웨어 보안

서버 및 데이터 뱅크는 보안 시스템의 일부입니다. 비록 이 책에서 하드웨어를 다루고 있지 않지만 서버와 보안 관리에 사용되는 워크스테이션의 물리적 보안을 계획해야 합니다.

Trust Authority 하드웨어 보안

비록 이 섹션은 특별히 Trust Authority 구성요소를 다루고 있지만 고려사항은 모든 FirstSecure 구성요소에 적용 가능합니다.

영역 격리

CA 활동 전용의 격리된 방에 서버를 설치합니다. 가능한 경우 방에는 강화된 벽, 단단한 나무 또는 강철 문 하나 그리고 떨어지는 판이 없도록 하나로 만들어진 천정이 있어야 합니다. 방에는 또한 화재가 났을 때 방전되지 않도록 바닥을 돋구어 놓아야 합니다.

영역 유지보수

방은 컴퓨터, 전등, 움직임 감지기 및 난방과 냉방 시스템에 무정전 전원

공급 장치(UPS)를 제공해야 합니다. 또한, 방의 통풍을 감사하여 장치에서 생기는 열을 이겨낼 수 있도록 온도를 유지해야 합니다.

영역에 대한 액세스 제어

배지나 키패드로 제어되는 문 열쇠를 사용하는 등의 여러 가지 방법으로 물리적 영역을 액세스를 제공할 수 있습니다. 한 개인이 고의로 장난치지 못하도록 하려면 최소한 신뢰할 수 있는 두 개인의 적합한 인증사항을 제시해야하는 제어를 설치해야 합니다.

또한, 방을 모니터하여 보안 영역에 누가 언제 들어 갔는지를 추적해야 합니다. 최대한의 보안을 위해 문 안팍에 움직임 감지기를 설치합니다.

제어 통신

Trust Authority 서버에는 여분의 열린 포트가 없어야 합니다. 시스템이 활성화된 Trust Authority 응용 프로그램에 명시적으로 할당된 포트에 대한 요청만 청취할 수 있도록 구성해야 합니다.

비지니스 절차와 e-business에서 사용되는 하드웨어 보안 요구사항을 따르십시오.

제4장 e-business 네트워크에서의 FirstSecure 계획

제2부에 있는 다음 장은 FirstSecure에 포함된 제품을 e-business에 연결합니다. 이 장은 19 페이지의 『제3장 e-business 네트워크 개요』의 그림 위에 구축됩니다. 각 제품은 자세히 설명되어 있습니다. 제품에 대한 완전한 정보를 얻으려면 제품과 함께 제공되는 문서를 참조하십시오. 전개 시나리오는 제안일뿐입니다.

각 전개 시나리오에서 같은 기본 단계를 수행하십시오.

1. 네트워크의 모든 부분이 공통 시간 참조를 사용하여 감사 로그를 더 간단하고 더 정확하게 만듭니다.
2. 인트라넷에서 시작하여 구성요소를 설치하고 테스트합니다.
3. 일단 인트라넷에 익숙해지면 보안 DMZ에서 응용 프로그램을 구축합니다.
4. 인트라넷과 DMZ(demilitarized zone)간의 트래픽은 Firewall을 통과해야 합니다.
5. 외부 인터넷 응용 프로그램을 구축하고 테스트 데이터를 사용하여 테스트합니다.
6. Firewall을 설치하여 인터넷과 DMZ간의 트래픽을 보호합니다.
7. 사용자가 네트워크를 액세스할 수 있게 합니다.

완전한 FirstSecure 시스템 계획

여기에는 네트워크에서 FirstSecure 제품을 전개하는 제안된 순서가 있습니다. 이는 아주 간단합니다. 각 제품에 대한 자세한 하드웨어 및 소프트웨어 요구사항과 통합 고려사항에 대해 59 페이지의 『제3부 설치 및 통합 고려사항』을 참조하십시오. 또한, 각 제품과 함께 제공되는 설치 요구사항과 지침을 읽으십시오. 많은 제품은 인터넷에서 얻을 수 있는 최신 정보도 있습니다. xiii 페이지의 『웹 정보』에는 FirstSecure 정보가 있는 웹 사이트가 있습니다. Redbook인 *Understanding the IBM SecureWay FirstSecure Framework*, SG24–5498에는 더 자세한 시나리오가 있습니다.

1. 필요한 보안 요구사항을 계획하십시오.
2. 이런 요구사항을 충족할 수 있도록 Policy Director를 설치하십시오.
3. 고객 서버 응용 프로그램을 만들고 테스트하십시오. 당분간 이를 사내 인트라넷에서 유지하고 아직은 인터넷에서 사용할 수 없게 만드십시오.
4. 고객 서버 응용 프로그램을 보호하는 IBM Firewall을 설치하십시오.
5. SurfinGate를 DMZ에 추가하십시오.
6. DMZ에서 MIMEsweeper와 Norton AntiVirus를 추가하여 인터넷에서 응용 프로그램을 사용할 수 있게 만들 때 이를 보호하십시오. 이를 외부 트래픽에서 사용할 수 있게 만들 때 서버를 가리키도록 구성하십시오.
7. 침입 방어 및 감지를 위해 Tivoli Cross-Site for Security 제품을 설치하십시오.
8. DMZ에서 다음을 추가하십시오.
   - 웹 서버
   - 웹 카탈로그 서버
   - 웹 재고 서버
   - 고객 클라이언트 응용 프로그램
   - 보안 고객 클라이언트 응용 프로그램
   - 하나 이상의 Cross-Site for Security 에이전트

   트래픽에 모든 응용 프로그램을 개방하기 전에 Firewall에서 이를 테스트하십시오. SecureWay Boundary Server의 네트워크 보안 감사기 툴을 사용하여 설정한 규칙을 테스트하십시오.
9. IBM SecureWay Firewall의 인스턴스를 설치하여 DMZ에 있는 소프트웨어를 보호하십시오. 기본 구성은 설치를 일반에게 개방하기 전에 이를 테스트할 수 있도록 『트래픽 없음』이어야 합니다.
10. Trust Authority를 설치하고 신뢰할 수 있는 사용자에게 인증서를 발급하십시오.
11. 모든 테스트가 끝난 다음 응용 프로그램을 인터넷에서 개방합니다.
12. 시스템 외부에서 네트워크 보안 감사기를 실행하여 일반에게 액세스를 허용하기 전에 규칙을 테스트하십시오.

13. 부적절한 사건이 없도록 FirstSecure 구성요소 프로그램에서 작성한 감사 로그를 확인하십시오.
14. 계속 감사 로그를 확인하고 응용 프로그램을 네트워크에 추가할 때 Cross-Site for Security 에이전트를 추가하십시오.

제5장 네트워크에서의 Policy Director 계획

FirstSecure는 이기종 웹 환경을 위한 강화된 정책 중심의 제어 포인트를 제공합니다. 사용자가 브라우저를 통해 여러 백-엔드 서버를 액세스할 수 있는 환경에서 Policy Director는 다음을 제공합니다.

- 각 웹 사용자를 위한 단일 사인온
- ID 검증
- 보호된 웹 페이지에 대한 액세스를 요청하는 사용자의 권한 부여 확인

이런 지원으로 다음에 대해 권한을 부여하고 안전하게 할 수 있습니다.

- HTML, 텔넷 및 POP3와 같은 TCP/IP 교환
- 데이터베이스 시스템과 같은 타사 응용 프로그램
- 네트워크 관리 툴
- 사내에서 개발된 응용 프로그램

FirstSecure를 이용하면 사용자는 다음 메커니즘으로 Policy Director를 인증할 수 있습니다.

- 보안 소켓 계층(SSL)을 통한 기본 인증
- SSL을 통한 양식 기반 로그인
- 클라이언트 인증서를 사용하는 SSL
- Kerberos 로그인

그런 다음 FirstSecure는 각 웹 오브젝트와 네트워크 서비스에 대한 인증된 사용자의 액세스를 제어하고 이들 자원의 서브세트에 대한 권한 없는 사용자를 제한할 수 있습니다.

Policy Director 전개

Policy Director는 사용자와 그룹 및 자원간의 맵핑을 관리합니다. Policy Director 관리 콘솔을 사용하여 다음을 수행합니다.

- 자원을 사용할 사용자와 그룹을 정의합니다.
- 보호가 필요한 오브젝트를 정의합니다. 오브젝트는 웹, TCP 포트, 메소드 및 인터페이스입니다.
- 사용자가 자원을 액세스하는 방법과 읽기, 수정, 관리, 실행 또는 삭제와 같이 자원을 보호하는 규칙을 정의합니다.

다음 표는 공통 Policy Director 구성요소 구성을 설명합니다. 네트워크에 적합한 구성을 결정하십시오. 그런 후 설치 중에 구성요소를 선택합니다.

더 자세한 내용은 *IBM SecureWay Policy Director Up and Running*을 참조하십시오.

구성 예제	설치된 구성요소
보안 도메인에 대해 관리 서버의 단일 인스턴스를 실행하는 서버. 이 시나리오에서 관리 서버는 자신의 시스템에 단독으로 상주합니다. 관리 서버는 보안 도메인에 대한 마스터 권한 부여 데이터베이스를 유지보수하고 보안 도메인 전반에 걸쳐 이 데이터베이스를 복제하며 보안 도메인에서 다른 Policy Director 서버 시스템에 대한 위치 정보를 유지보수합니다.	관리 서버 전용
WebSEAL 서버. 이 시나리오는 웹 공간을 보호하는 솔루션을 나타냅니다. WebSEAL은 높은 가용성과 결함 허용 한계를 위해 백엔드 서버를 지원합니다.	WebSEAL이 있는 보안 관리자
NetSEAL 서버. 이 시나리오는 VPN(Virtual Private Network)을 보안하는 솔루션을 나타내고 레거시와 타사 네트워크 서비스에 대해 액세스 제어를 제공합니다.	NetSEAL이 있는 보안 관리자
WebSEAL과 NetSEAL 서버 조합.	WebSEAL과 NetSEAL이 있는 보안 관리자

구성 예제	설치된 구성요소
타사 응용 프로그램에 대해 Policy Director 권한 부여 서비스에 대한 액세스를 제공하는 서버.	권한 부여 서버
권한 부여 API를 사용하는 기타 응용 프로그램을 구축하는 개발자를 위해 개발 환경을 제공하는 서버.	권한 부여 서버 및 ADK
위의 모든 구성의 조합된 서비스를 제공하는 서버.	모든 구성요소

Policy Director는 하나 이상의 시스템에서 다양한 구성으로 그 구성요소를 전개할 수 있는 널리 분배된 보안 시스템입니다. 다음은 네트워크에서 이루어지는 Policy Director 전개 개요입니다. 완전한 설치 지침은 *IBM SecureWay Policy Director Up and Running*에 있습니다.

1. Policy Director 보안 서버를 설치하십시오.

   Policy Director 보안 도메인을 설치하기 위해 보안 도메인에 있는 컴퓨터 중 최소한 하나에는 Policy Director 보안 서버가 있어야 합니다. 필수 플랫폼에 대해 설치 및 관리 안내서와 기술 지원 자원을 참조하십시오.

   나머지 서버는 DCE 클라이언트 설치(또는 Windows NT 시스템의 NetSEAT에서)에서만 기능할 수 있습니다.

2. SecureWay Directory(LDAP) 서버를 설치하십시오.
3. Policy Director를 설치하십시오.
   - Policy Director 보안 서버를 먼저 전개하십시오(1 단계 참조하십시오).
   - 모든 Policy Director 서버 설치에는 Policy Director Base가 필요합니다.
   - 이것이 보안 도메인에서 *첫번째*이거나 *유일한* 시스템이면 관리 서버를 설치해야 합니다.

     기존 관리 서버가 있는 기존 보안 도메인에서 이것이 *추가* 시스템이면 다른 관리 서버를 설치하지 마십시오. 주어진 보안 도메인에는 관리 서버의 인스턴스가 하나뿐이어야 합니다.
   - WebSEAL, NetSEAL 및 타사 권한 부여 서버 구성요소는 선택적입니다.
   - 보안 관리자는 WebSEAL과 결합하여 WebSEAL HTTP 서버 구성요소와 잘 조정된 HTTP 액세스 제어를 제공하고, NetSEAL과 결합하여 대략적인 NetSEAL TCP/IP 액세스 제어 구성요소를 제공합니다.
4. 관리 콘솔을 설치하십시오.

관리 콘솔에서는 운영 체제에서 DCE 클라이언트(또는 Windows NT용 NetSEAT)를 설치해야 합니다(37 페이지의 1 단계 참조하십시오).

5. 다음 종속성은 권한 부여 ADK로 개발된 응용 프로그램에 적용됩니다.
   - Policy Director 패키지가 필요합니다.
   - 응용 프로그램 시스템에 IVAuthADK를 설치하십시오.
   - 응용 프로그램이 실행해야 하는 운영 체제에는 DCE 클라이언트나 Windows NT 시스템용 NetSEAT가 있어야 합니다.
   - 응용 프로그램을 실행하는 보안 도메인에는 보안 도메인의 컴퓨터 중 최소한 하나에 설치된 권한 부여 서버가 있어야 합니다. 일반적인 개발 환경에는 권한 부여 ADK와 같은 운영 체제에 있는 권한 부여 서버가 있습니다.

제6장 네트워크에서의 SecureWay Boundary Server 계획

FirstSecure는 SSL(Secure Sockets Layer), SOCKS 및 IPSec과 같은 기존 보안 표준을 사용하는 웹 기반 응용 프로그램에 보안을 제공합니다.

작업 환경이 신뢰 특성이 다른 네트워크의 두 부분 간에 연결을 포함하는 경우 FirstSecure의 SecureWay Boundary Server 구성요소는 다음 요구사항을 지정하는 데 도움이 될 수 있습니다.

- 인터넷으로의 안전한 연결, 개인 네트워크로의 권한 없는 액세스 가능성을 최소화
- 비지니스 파트너 및 공급업체와 선택적인 데이터 공유를 위한 대형 익스트라넷 하부구조
- 인터넷 또는 기타 관련된 신뢰되지 않은 네트워크 세그먼트를 VPN(virtual private network)로 사용하며, 이때 메시지는 신뢰되지 않은 네트워크의 하부구조를 통해 통과하는 동안 기밀이 보존됩니다.

FirstSecure의 SecureWay Boundary Server는 네트워크 주소 필터링, 내용 필터링 및 회선 레벨 게이트웨이 기술을 사용합니다 이러한 기술을 결합하여 사용하면 SecureWay Boundary Server는 신뢰 특성이 다른 네트워크간의 통신을 제어함으로써 정책 중심의 안전한 보안 e-business 작동을 방침 위주로 안전하게 할 수 있게 됩니다.

SecureWay Boundary Server에는 다음을 포함합니다.

- IBM SecureWay Firewall, ACE/Server 포함
- IBM SecureWay 릴리스 2용 MIMEsweeper
- Windows NT용 SurfinGate 4.05
- 정책 관리 개선사항

완전한 SecureWay Boundary Server 설치에서의 데이터 흐름의 개요에 대해서는 40 페이지의 그림10을 참조하십시오.

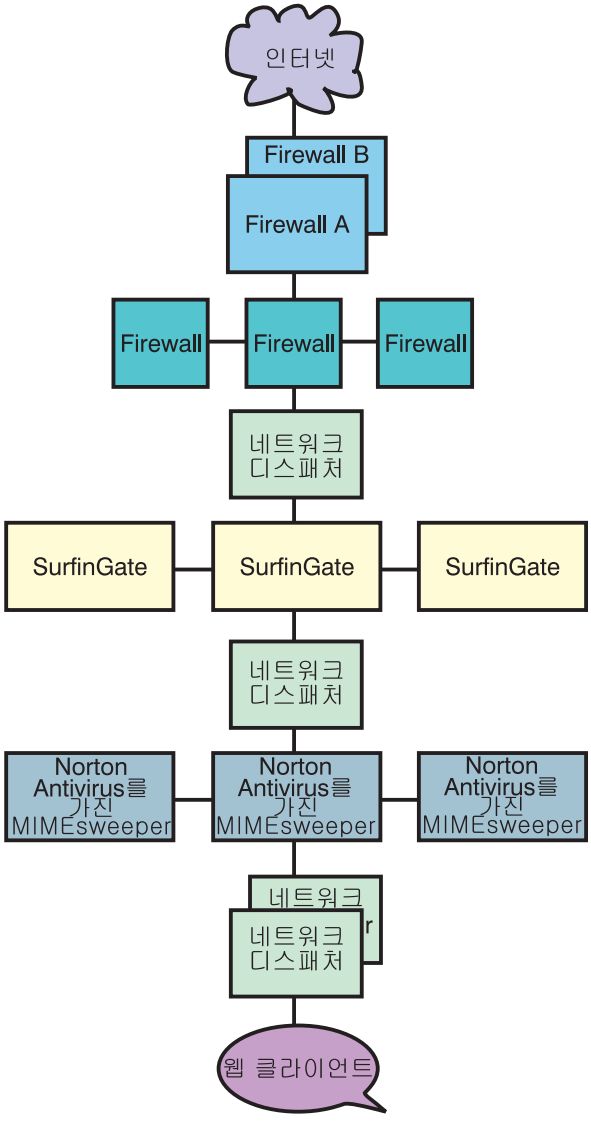


그림 10. SecureWay Boundary Server 제품에서의 데이터 흐름 개요

IBM SecureWay Firewall 전개

IBM Firewall이라고도 하는 IBM SecureWay Firewall은 인터넷과의 통신을 제어합니다. 이 Firewall 기술은 IBM 자산을 보호합니다.

설치 고려사항에 대해 67 페이지의『SecureWay Boundary Server 구성요소 고려사항』을 참조하십시오.

네트워킹 고려사항 중에는 다음이 포함됩니다.

- 인터넷과 연결은 필요하지만 사내 네트워크, 응용 프로그램 및 데이터에 권한 없는 액세스를 차단합니다.
- 내부 사용자에 의한 사내 네트워크 자산 오용
- 구성 관리의 고비용에도 불구하고 비지니스 파트너 및 공급업체를 위한 대규모의 엑스트라넷 하부구조 계획 방법
- 지사를 연결하는 전용 회선의 높은 비용
- 파트너와 공급업체 간의 비효율적이고 느리며 상호 잘못 이해되는 통신으로 인한 낮은 비지니스 생산성
- 자연어가 아닌 소프트웨어 관리의 높은 관리 비용

IBM Firewall은 이러한 고려사항에 대해 지적합니다. 확실히 허용된 트래픽만을 Firewall에서 허용함으로써, IBM Firewall은 외부인으로부터 네트워크를 보호합니다. 더 나은 보호를 위해, IBM Firewall에 들어있는 취약점 점검 소프트웨어는 IBM Firewall이 실행되고 있는 서버를 *강화*하여 해커가 Firewall에 또는 통해서 들어올 수 없도록 할 수 있습니다. 내부 네트워크의 IP 주소와 구성은 신뢰되지 않은 네트워크에서 숨겨집니다. Firewall을 통한 모든 트래픽은 로그되어 사용자 활동 보고서를 작성하는 데 사용될 수 있습니다.

IBM Firewall 및 그 VPN 구성 응용 프로그램을 사용하면 대형 VPN 하부구조를 전개하고 저비용으로 관리할 수 있습니다. 네트워크에 대한 연구에서는 고객이 VPN을 사용하면 전용 회선 솔루션의 비용을 상당히 많이 절약할 수 있음을 보여주고 있습니다.

IBM Firewall을 사용하면 각 지사에 Firewall을 전개하고 IPSec 기반 터널을 사용하여 인터넷을 통해 지사와 서로 연결할 수 있습니다.

IBM Firewall은 Security Dynamics Technology사의 제품인 ACE/Server와 함께 제공됩니다. ACE/Server는 권한 부여 받은 사용자만 네트워크 파일, 응용 프로그램 및 통신을 액세스할 수 있도록 엔터프라이즈 네트워크에 대해 강력한 중앙 집중 인증 서비스를 제공합니다. Security Dynamics Technologies 사의 특허가

있는 SecurID 토큰 기술을 사용하여 ACE/Server는 권한 없는 액세스에 대해 하나의 울타리를 작성합니다. 인증은 두 가지 요인 즉, 사용자가 무언가(SecureID 토큰 카드)를 *가지고* 있으며 인증 받아야 하는 무언가(PIN)를 알고 있는지에 따라 이루어집니다.

MIMEsweeper 전개

MIMEsweeper는 Content Technologies 사의 제품으로서 인터넷과 인트라넷의 내용기준 분석을 수행하여 숨겨진 모든 위협을 식별해 내고 이런 위협으로부터 네트워크 사용자를 보호합니다.

설치 고려사항에 대해 67 페이지의 『SecureWay Boundary Server 구성요소 고려사항』을 참조하십시오.

MIMEsweeper에는 2개의 기본 모듈 MAILsweeper 및 WEBsweeper가 있어서 다른 방식으로 사용자를 보호합니다. 메일 및 기타 웹 데이터가 MIMEsweeper에 입력되면, MIMEsweeper는 송신자와 수신자의 주소를 검증하고 구성요소 부분으로 파일을 분해합니다. MAILsweeper 및 WEBsweeper는 그런 다음 이들 부분을 분석하여 개인 네트워크를 위협할 수 있는 위험을 취소화합니다.

FirstSecure에는 MAILsweeper 4.0과 WEBsweeper 3.2_5가 둘 다 있습니다. 각각은 따로 설치, 구성 및 사용할 수 있습니다.

MAILsweeper는 다음을 수행할 수 있습니다.

- 분해한 파일들에 바이러스가 없는지 확인하기 위해 선택한 바이러스 스캐너와의 작업
- 매크로 폭탄 감지 및 블록화
- 다음을 위한 키워드 검색
  - 전자 우편에서 골칫거리나 저속한 언어에 대한 보호
  - 중요한 데이터가 회사 밖으로 유출되지 않도록 보호
- 수신되는 전자 우편 스팸을 블록화하여, 네트워크가 혼잡하지 않도록 하고 사원의 생산성 유실을 최소화

- AVI 또는 MPEG과 같은 일정한 유형의 파일 전송 또는 수신으로부터 개인 또는 그룹 블록화
- 네트워크가 트래픽을 보다 잘 허용할 수 있을 때까지 기본 크기로 파일 블록화 또는 지연

WEBsweeper는 다음을 수행할 수 있습니다.

- 작업과 관련없는 일련의 사이트 제어
- 기밀 또는 중요한 문서의 부주의한 유실 보호

추가적으로 MIMEsweeper에는 타사 URL 블록커를 통합하는 데 사용할 수 있는 API가 들어 있습니다.

MIMEsweeper는 회사 및 사용자들을 인터넷의 보안 위험으로부터 보호하는 중요한 자산입니다.

주: 비록 MIMEsweeper 문서에서 서비스와 지원을 받기 위한 Content Technologies 문의처를 제공하지만 IBM SecureWay 릴리스 2용 MIMEsweeper를 SecureWay FirstSecure 제품이나 SecureWay Boundary Server 제품의 일부로 구입하는 경우에는 IBM에 문의해야 합니다.

SurfinGate 전개

SurfinGate는 Finjan Software Ltd.의 제품으로서 JavaScript 코드, Java 애플릿 및 ActiveX 제어와 같은 모빌 코드를 조사하여 데이터 수정, 정보 삭제 및 부정 데이터 수집과 같은 손상으로부터 네트워크를 보호합니다. SurfinGate는 게이트웨이 레벨에서 모빌 코드를 점검하고 네트워크에 입력하기 전에 위험한 코드를 식별합니다. 모빌 코드는 사용자 또는 부서별로 선택적으로 블록화되거나 허용될 수 있으며, 코드는 의도하는 기능에 따라 사내 네트워크로의 액세스가 허용되거나 거부될 수 있습니다. SurfinGate를 사용하면 관리자가 ActiveX, Java, JavaScript, Visual Basic Script, 플러그 인 및 쿠키에 대한 코드를 사용할 수 있으며 회사 전체의 보안 정책을 관리, 제어 및 실행할 수 있습니다.

SurfinGate에는 다음과 같은 구성요소가 있습니다.

- SurfinGate 서버

- SurfinConsole
- SurfinGate 데이터베이스
- WTE 통합용 플러그인

SurfinGate 서버는 HTTP 프록시 서버로서 또는 Firewall나 프록시의 서비스로서 작동합니다. SurfinGate 서버는 회사 Firewall과 기존의 기타 프록시 다음에 배치할 수 있으며 HTTP 서버로도 작동할 수 있습니다. 이 구조에서는 침입이 발생하기 전에 모빌 코드 트래픽을 중지하고 점검할 수 있습니다.

네트워크 관리자는 SurfinConsole을 사용하여 모벨 코드에 대해 중앙 보안 정책을 관리하고 설정합니다. SurfinConsole은 네트워크에 있는 여러 SurfinGate 서버를 제어하고 사용자나 그룹별로 회사 전체에서 또는 허용불능/허용가능 코드의 사용자 정의 목록을 통해 모빌 코드 규칙을 강제 실행할 수 있습니다.

SurfinGate 데이터베이스는 ASPs(Applet Security Profiles)의 상세내용을 저장하며, 여기에는 사용자 및 그룹에 대한 정보와 해당 보안 정책이 포함됩니다. SurfinGate는 모든 모빌 코드의 내용을 동적으로 점검하므로, 데이터베이스는 보안이 필요없지만 대규모 조작에서의 성능을 향상시키는 데 도움이 됩니다.

주: 비록 SurfinGate 문서에서 서비스 및 지원을 받기 위한 Finjan 문의처를 제공하지만 SecureWay FirstSecure 제품 또는 SecureWay Boundary Server 제품의 일부로 Windows NT용 SurfinGate를 구입한 경우에는 IBM에 문의해야 합니다.

제7장 네트워크에서의 Intrusion Immunity 계획

지금까지 설명한 보안 기술은 보안 위협으로부터 보호하는 것에 중점을 두었습니다. 보안에서 이에 못지 않게 중요한 것은 위협의 감지입니다. FirstSecure의 침입 방지 제품은 회사에서 보안 위협을 감지할 수 있도록 침입 감지와 antivirus 기능을 제공합니다.

바이러스 방지 소프트웨어는 트로얀의 말, 웜, 매크로 바이러스, 불량의 ActiveX 제어 및 불량의 Java 애플릿을 포함하는 모든 종류의 유해한 코드로부터 보호합니다. 바이러스 보호는 모든 보안 솔루션의 필수 부분입니다. FirstSecure의 Antivirus 제품에서는 이러한 핵심적인 antivirus 요구사항을 지적합니다.

- 고정 및 모빌 클라이언트의 antivirus 요구에 대한 포괄적이고 일관성 있게 접근하기 위한 광범위한 클라이언트 세트 적용범위.
- 바이러스 특성에 대한 등록 서비스. 정기적으로 바이러스 특성을 갱신하는 것은 유해한 코드에 대해 효과적으로 보호하기 위해서는 중요합니다.
- 바이러스 방지 정책이 실행되는지를 확인하기 위한 서버에서 클라이언트로의 antivirus 갱신의 정책 중심의 분배.

Tivoli Cross-Site for Security 전개

Tivoli Cross-Site for Security는 공격하기 쉬운 시스템에 네트워크 기반 침입 감지 기능을 제공합니다. 관리 도메인이 인터넷에 연결되는 위치마다 Tivoli Cross-Site for Security 에이전트를 전개할 수 있습니다. Tivoli Cross-Site for Security는 네트워크를 모니터하여 내부 및 외부 공격을 감지합니다. 이는 다음과 같은 이득을 제공합니다.

- Cross-Site for Security 관리자에게 잠재적 공격을 경보해 주는 실시간 침입 감지
- DMZ에 있는 에이전트와 인트라넷의 에이전트에 서로 다른 정책을 설정할 수 있게 하는 구성 가능한 정책
- 급변하는 환경에 빨리 응답할 수 있게 하는 보안 에이전트 정책의 온라인 수정

- Tivoli 엔터프라이즈 관리 시스템을 늘릴 수 있도록 하는 Tivoli의 엔터프라이즈 응용 프로그램과의 통합

Tivoli Cross-Site for Security는 다음과 수행할 수 있습니다.

- 스캔과 홍수(flood) 발견
- IP 트래픽 모니터
- 포트 서비스 모니터
- DNS, 마운트 서비스 및 네트워크 파일 시스템 요청 및 응답 발견
- Portmapper 서비스 요청 및 응답 덤프 발견
- RStatd 호출 발견
- 특정 맵 이름과 파일 이름에 대한 요청 발견
- PC 파일 서버에서 SMB 기반 공격 발견
- 인터넷 제어 메시지 프로토콜 발견

Cross-Site for Security를 사용하여 네트워크 트래픽을 모니터하고 공격과 침입 시도를 발견합니다. 이는 인터넷에서 인트라넷을 격리시키는 DMZ와 내부 네트워크에서 트래픽을 모니터합니다.

Cross-Site for Security에서 발견할 수 있는 침입 유형에는 다음이 포함됩니다.

- 서명 또는 패턴, 발견
- 홍수(flood) 발견
- 네트워크 기반 공격
- Windows 네트워크 공격
- 원격 절차 공격
- 서비스 사용
- 권한없는 네트워크 트래픽
- 의심 가는 활동

Cross-Site for Security는 Cross-Site for Security 에이전트와 Cross-Site for Security 관리 서버를 사용하여 네트워크를 보호합니다. 에이전트에서 심각한 공격을 발견하면 즉시 정보를 로그하고 응답하는 Cross-Site for Security 관리 서

버로 암호화된 이벤트를 전송합니다. Cross-Site for Security 관리 서버를 구성하여 경보를 콘솔로 보내고 이메일을 관리자에게 보내거나 호출할 관리자에게 페이저를 보냅니다.

Tivoli Cross-Site for Security 라이센스 키 확보

Tivoli Cross-Site for Security 제품을 사용하려면 라이센스 키를 사용자 정의해야 합니다.

Tivoli Cross-Site 웹 사이트로 가서 다음 단계를 완료하면 라이센스 키를 수신할 수 있습니다.

1. Tivoli Cross-Site for Security CD-ROM이 포함된 FirstSecure 제품과 함께 제공되는 Passport Advantage Proof of Entitlement 문서와 *Tivoli Cross-Site for Security Installation*을 찾습니다.
2. Passport Advantage Proof of Entitlement에서 8자리 숫자로서 5로 시작하는 주문 번호와 7자리 숫자로서 7로 시작하는 고객(사이트) 번호를 찾습니다. 이런 번호를 사용하여 Tivoli Cross-Site 웹 사이트를 액세스합니다.
3. 맨처음 인터넷을 액세스할 수 있는 컴퓨터의 웹 브라우저를 사용하여 Tivoli Cross-Site 웹 사이트에 로그인합니다. 웹 사이트의 URL은 `www.cross-site.com/support/licensing/`입니다.
4. 주문 번호, 고객 번호 및 문의처 번호를 입력합니다. Tivoli Cross-Site for Security를 설치할 서버의 도메인 이름도 제공해야 합니다.
5. 웹에서 추가 지침을 따릅니다.
6. Tivoli Cross-Site 라이센스 키 웹 사이트를 액세스하는데 문제가 있으면 1–800–2–TIVOLI, 교환 9396의 Tivoli Cross-Site 지원에 문의하거나 licensing@cross-site.com으로 이메일합니다.

관련 Tivoli Cross-Site 제품

Tivoli Cross-Site 제품 계열에는 FirstSecure 계열의 일부가 아닌 기타 구성요소가 있습니다.

- Tivoli Cross-Site for Avaliability는 일반 사용자가 웹 사이트를 성공적으로 액세스할 수 있는지를 모니터하고 보고합니다.

- Tivoli Cross-Site for Deployment는 엔터프라이즈의 범위를 확장하여 인터넷을 통해 중요한 응용 프로그램과 정보를 분배하고 관리할 수 있습니다.

비록 이런 제품은 Tivoli Cross-Site for Security 문서에서 언급되지 않아도 별도로 구입해야 합니다.

Tivoli Cross-Site for Security를 사용하여 트래픽 모니터

Cross-Site for Security 에이전트는 지능형 네트워크 탐지기입니다. 이는 계속 네트워크에서 패킷을 모니터합니다. Cross-Site for Security 에이전트는 이런 패킷을 필터하여 의심 가는 활동을 나타내는 다양한 서명을 찾아봅니다. 이런 서명은 네트워크 공격을 나타냅니다.

Cross-Site for Security 에이전트는 UNIX에서 *디먼*으로 실행하고 Windows NT에서 NT 서비스로 실행합니다. Cross-Site for Security는 시스템이 부트할 때 자동으로 시작하도록 구성됩니다. 이는 계속 상주해 있으면서 사용자의 로그인 여부와 관계없이 시스템 백그라운드에서 실행합니다.

잠재적 공격이 발견되면 에이전트는 심각도를 판별하고 즉시 관리 서버에 알릴 것인지 아니면 경보를 로컬 파일에 로그할 것인지를 판별합니다. 로그는 정기적으로 관리 서버에 업로드됩니다.

에이전트는 또한 정기적으로 Cross-Site for Security 관리 서버에 접속하여 에이전트가 활성화되어 있으며 실행 중임을 알립니다. 이런 유형의 통신을 *하트비트*라고 합니다. 하트비트 간격을 구성할 수 있습니다.

관리 서버가 에이전트에서 하트비트를 수신하면 관리 서버는 에이전트에게 갱신된 구성 정보, 새 서명 및 업로드 스케쥴을 알립니다. 에이전트는 자동으로 이런 갱신을 다운로드하고 설치합니다.

네트워크에서의 Tivoli Cross-Site for Security

Cross-Site for Security가 비지니스 요구사항에 맞도록 구성할 수 있습니다. 주요 결정은 다음과 같습니다.

- Cross-Site for Security 관리 서버를 설치할 위치
- 필요한 Cross-Site for Security 에이전트의 수

- Cross-Site for Security 에이전트를 설치할 위치

크기, 토폴로지 및 네트워크 대역폭과 트래픽 외에 이런 고려사항은 관리 서버와 에이전트 수를 결정하는데 있어서 중요합니다. Tivoli Cross-Site for Security 설치 고려사항에 대해 73 페이지의 『Intrusion Immunity 하드웨어 및 소프트웨어 요구사항』을 참조하십시오.

주: 비록 Tivoli Cross-Site for Security 문서에서 서비스와 지원을 설명해도 Tivoli Cross-Site for Security를 SecureWay FirstSecure 제품의 일부로 구입하는 경우에는 IBM에 문의해야 합니다.

Norton AntiVirus 전개

Symantec Corporation의 제품인 Norton AntiVirus는 세계적인 antivirus 소프트웨어 제품 중 하나입니다. Norton AntiVirus는 다음과 수행할 수 있습니다.

- 감염된 파일을 격리합니다
- 바이러스와 불량의 ActiveX 제어 및 Java 애플릿으로부터 보호합니다
- 이메일 첨부, 인터넷 다운로드, 플로피 디스크, 소프트웨어 CD 또는 네트워크에서 들어 올 수 있는 바이러스로부터 보호합니다

Norton AntiVirus가 컴퓨터를 안전하게 지키기 위해 백그라운드에서 계속 실행하도록 스케쥴할 수 있습니다. Symantec 연구진은 Norton AntiVirus가 발견할 수 있는 바이러스를 계속 추가하고 있습니다. LiveUpdate 기능을 사용하여 일주일에 한번씩 Symantec에서 새로운 antivirus 정의를 자동으로 검색할 수 있습니다.

Norton AntiVirus의 격리 기능은 감염되었거나 의심이 가는 파일을 다른 파일과 분리하여 컴퓨터의 안전한 위치에 격리시킴으로써 파일을 수정하는 동안 바이러스의 확산을 막을 수 있습니다.

스캔 및 전달 마법사를 사용하면 의심이 가는 파일을 검사하기 위해 Symantec으로 보낼 수 있습니다. SARC(Symantec AntiVirus Research Center)는 문제를 해결할 수 있도록 응답합니다.

Norton AntiVirus 스캐너인 *Bloodhound*는 백그라운드에서 실행하여 새 바이러스에 감염될 가능성이 있는 응용 프로그램의 동작을 관찰하고 분류합니다. 응용 프

로그램이 바이러스처럼 작동하고 다른 프로그램을 감염시키려고 하면, Bloodhound가 프로그램을 중단시켜 새로운 바이러스 갱신을 받을 때까지 다른 파일들의 감염을 예방할 수 있습니다.

FirstSecure에서 제공하는 Norton AntiVirus Solution Release 3.04 제품은 다음과 같습니다.

- 데스크탑 솔루션:
  - Norton AntiVirus 4.08 for DOS
  - Norton AntiVirus 4.08 for Windows 3.51
  - Norton AntiVirus 5.02 for Windows 95/98
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 5.03 for Macintosh
  - Norton AntiVirus 5.02 for OS/2
- 서버 솔루션:
  - Norton AntiVirus 4.08 for Windows NT 3.51
  - Norton AntiVirus 5.02 for Windows NT 4.0
  - Norton AntiVirus 4.04 for NetWare
  - Norton AntiVirus 2.0 for Lotus Notes™ and OS/2
  - Norton AntiVirus 1.52 for Microsoft Exchange
- 게이트웨이 솔루션:
  - Norton AntiVirus 1.02A for Internet E-mail Gateways for NT
  - Norton AntiVirus 1.04 for Firewalls
- 관리:
  - Norton System Center 3.1
  - Norton AntiVirus 5.03 for Macintosh Administrator
  - Norton AntiVirus Plus 5.0 for Tivoli Enterprise
  - Norton AntiVirus Plus 5.0 for Tivoli IT Director
  - 기타 관리 도구 - Norton AntiVirus Network Manager (NAV32/NAVNETW) v3.01

Norton AntiVirus에 대한 자세한 내용은 Norton AntiVirus CD의 루트 디렉토리에 있는 contents.txt 파일에 있습니다.

주: 비록 Norton AntiVirus 문서에서 서비스 및 지원을 받기 위한 Symantec 문의처를 제공하지만 Norton AntiVirus Solution Release 3.04를 SecureWay FirstSecure 제품의 일부로 구입하는 경우에는 IBM에 문의해야 합니다.

상세한 설치 단계에 대해서는 특정 제품과 함께 제공되는 문서와 73 페이지의 『제 13장 Intrusion Immunity 요구사항 및 설치 고려사항』의 하드웨어 및 소프트웨어 요구사항을 참조하십시오.

제8장 네트워크에서의 공용 키 하부구조 계획

공용 키 하부구조의 Trust Authority 구성요소는 사용자를 인증하고 신뢰할 수 있는 통신을 보장하여 인터넷 응용 프로그램을 제공합니다. 암호화와 상호 조작 가능성에 대한 PKI(public key infrastructure) 표준 위에 구축된 Trust Authority 시스템은 디지털 인증서를 발급, 게시 및 관리하는 데 필요한 하부구조를 제공합니다. 여기에는 다음이 포함됩니다.

- IBM AIX 및 Microsoft Windows NT 서버 플랫폼에 대한 지원.
- 사용자 등록 다음에 관리 작업을 처리하는 RA(Registration Authority). 자동 프로세스나 사람의 의사 결정으로 구현될 수 있는 이 관리에는 다음과 같은 유형의 작업이 이루어집니다.
  - 사용자 ID 확인
  - 인증서를 확보, 갱신 또는 거부하는 요청을 승인 또는 거부
  - 사용자가 인증서의 공용 키에 관련된 개인 키를 가지고 있는지 검사
  - 주어진 비지니스 프로세스나 인증서 프로파일의 규칙을 따라 특정 유형의 사용자에게 특정 유형의 인증서를 발급

  RA 또한 인증서에 대한 정보를 통합된 공용 키 디렉토리인 IBM SecureWay LDAP 디렉토리에 게시합니다.
- 신뢰할 수 있는 CA(Certificate Authority). CA에서는 다음을 수행합니다.
  - 디지털 인증서를 발급하고 인증서를 인증하는 디지털 키 쌍을 생성합니다
  - 초기 등록에서 인증서 갱신 및 거부까지의 완전한 인증서 수명을 지원합니다
  - RA는 인증서가 거부되면 즉시 디렉토리를 갱신합니다
  - IBM SecureWay 4758 PCI Cryptographic Coprocessor 및 스마트 카드와 같은 암호화 하드웨어를 사용하여 키를 보호하도록 그 기능을 확장할 수 있습니다

- 브라우저 인증서, 서버 인증서 및 스마트 카드와 같은 특정 장치에 대한 인증서를 쉽게 확보할 수 있게 만드는 웹 기반 등록 인터페이스인 Credential Central. 관리자는 또한 이런 등록 양식을 사용하여 일반 사용자를 PKIX 인증서에 대해 사전에 등록할 수 있습니다.
- 사용자가 웹 브라우저를 사용하지 않고 PKIX 인증서를 확보, 갱신 및 거부할 수 있게 하는 독립형 Windows 인터페이스인 Trust Authority 클라이언트.
- 인간 관리자가 인증서를 확보, 갱신 또는 거부하기 위해 요청을 승인하거나 거부할 수 있게 하는 웹 기반 관리 인터페이스인 RA 데스크탑.
- 메시지 인증 코드(MAC)를 사용하여 Trust Authority RA 및 CA에서 수신한 이벤트를 인증할 수 있도록 하는 감사 서브 시스템. 구성 가능한 옵션을 통해 감사 레코드가 로그될 때 그 통합성을 보호할 수도 있습니다.
- 시스템 구성, 보안 암호 변경, CA 상호 인증, 통합성 확인 감사 로그 및 시스템 구성요소의 안전 시작과 중지를 위한 여러 관리 인터페이스.
- 응용 프로그램 개발자가 사용자 정의 PKI 응용 프로그램을 작성할 수 있게 하는 응용 프로그래밍 인터페이스(API).
- 통합된 IBM DB2 Universal Database의 런타임 지원. IBM SecureWay Directory 및 RA, CA 및 감사 구성요소마다 별도의 데이터베이스가 있습니다.

Trust Authority 전개

상세한 계획 및 설치 정보에 대해 *IBM SecureWay Trust Authority Up and Running*을 참조하십시오. 이 책에는 Windows NT 서버와 AIX에서 이루어지는 설치 시나리오와 단계가 있습니다.

제9장 엔터프라이즈에서의 SecureWay Toolbox 계획

네트워크가 아닌 개발 환경에서 FirstSecure Toolbox를 설치하도록 계획하십시오. 응용 프로그램을 외부 사용자에게 제공하기 전에 개발 환경에서 테스트하십시오.

권한 부여 서비스

권한 부여 서비스를 사용하면 웹 사이트를 액세스할 수 있는 권한을 부여 받은 사용자를 모니터할 수 있습니다. 인증은 암호나 공용 키를 기반으로 합니다. 이런 수단은 사이트에 있는 데이터의 통합성과 기밀성을 보호합니다. 권한 부여 서비스는 사용자 사이트에 있는 오브젝트를 액세스할 수 있는 자와 그 오브젝트를 액세스할 수 있는 방법을 정의하는 액세스 제어 목록(ACL)을 작성합니다. 권한 부여 서비스는 또한 보호된 오브젝트를 정의하고 단일 사인온에 대해 암호를 작성할 수 있게 합니다. 모든 보안 툴은 중앙 집중되므로 보안 정책을 쉽게 관리할 수 있습니다. 권한 부여 서비스는 IBM SecureWay Policy Director 권한 부여 API로 지원됩니다.

인증 권한 서비스

인증 권한 서비스는 X.509 Public Key Infrastructure for Multiplatforms 및 IBM KeyWorks Toolkit에서 지원됩니다.

인증 권한 서비스를 사용하여 디지털 인증서 관리를 통해 보안을 보장할 수 있습니다. 이런 서비스에는 인증서의 완전한 수명인 발급, 갱신 및 거부에 대한 API가 들어 있습니다. 이는 또한 인증서 거부 목록을 게시합니다. API는 공용 키 암호화와 스마트 카드 기술을 인증서 사용자를 인증하는 수단으로 사용합니다.

PKIX라고도 하는 X.509 Public Key Infrastructure for Multiplatforms는 PKIX API를 통해 제공됩니다. 이런 API를 사용하여 EE(end entity), CA(certificate authority) 및 RA(registration authority) 구성요소를 통해 인증서를 작성, 저장, 분배 및 거부할 수 있습니다. API는 IBM SecureWay Trust Authority와 인터페이스할 수 있도록 작동되며 IBMKeyWorks를 기반으로 합니다.

PKIX API에 대한 내용은 *IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference*를 참조하십시오. IBM KeyWorks에 대한 자세한 내용은 93 페이지의 『제16장 FirstSecure에서 제공하는 문서』에서 Toolbox와 함께 제공되는 문서 목록을 참조하십시오.

디렉토리 서비스

디렉토리 서비스는 IBM SecureWay Directory 클라이언트에 의해 지원됩니다.

디렉토리 서비스는 Lightweight Directory Access Protocol(LDAP)을 사용하여 디렉토리를 구성, 제어 및 액세스합니다. 이런 서비스는 LDAP 서버에 클라이언트 액세스를 제공하는 클라이언트/서버 모델을 기반으로 합니다. 디렉토리 서비스는 중앙 위치에서 디렉토리 정보를 저장, 갱신, 검색 및 교환하기 위해 유지보수하는 수단을 제공합니다. 디렉토리 서비스는 SSL(Secure Sockets Layer)를 사용하여 정보를 암호화합니다.

디렉토리 서비스에 대한 자세한 정보는 93 페이지의 『제16장 FirstSecure에서 제공하는 문서』에서 Toolbox와 함께 제공되는 완전한 IBM SecureWay Directory Client 문서 목록을 참조하십시오.

KeyWorks 암호화 및 신뢰 관리 서비스

암호화 및 신뢰 관리 서비스는 KeyWorks라고도 하는 IBM KeyWorks Toolkit에서 지원됩니다.

KeyWorks 암호화 및 신뢰 관리 서비스는 정보를 암호화하고 해독하여 정보를 액세스할 수 있는 사람을 제어합니다. 이런 서비스는 디지털 서명을 작성하고 확인하여 개인과 네트워크 컴퓨터의 ID를 인증합니다. 키를 분배하지 않고 암호화된 정보를 복구하는 키 복구 시스템은 IBM Key Recovery Service Provider에 통합됩니다.

KeyWorks는 암호화 및 신뢰 서비스 툴킷입니다. 이는 여러 계층의 보안 서비스 세트와 통합된 정보 세트 및 통신 보안 기능을 갖춘 관련 프로그래밍 인터페이스로 구성됩니다. 각 계층은 바로 밑에 있는 좀더 기본적인 서비스 계층에 구축됩니다. 이런 계층은 암호화 알고리즘, 난수 및 하위 계층의 고유한 식별 정보와 같은

기본적인 구성요소로 시작하고 상위 계층에서는 디지털 인증서, 키 관리와 복구 메커니즘 및 보안 트랜잭션 프로토콜을 구축합니다.

KeyWorks는 NLS(National Language Support)에 대해 작동되는데, 이는 제품이 언어, 스크립트, 문화 및 코드화된 문자 세트에 종속되어 있지 않다는 것을 의미합니다.

KeyWorksC API에 대한 자세한 내용은 93 페이지의 『제16장 FirstSecure에서 제공하는 문서』에서 Toolbox와 함께 제공되는 KeyWorks 문서 목록을 참조하십시오.

SSL(Secure Sockets Layer) 프로토콜 서비스

SSL(Secure Sockets Layer) 프로토콜 서버는 IBM SSL(Secure Sockets Layer) Toolkit에서 지원됩니다.

SSL 프로토콜 서비스는 데이터를 액세스할 수 사람을 결정할 수 있게 합니다. 이런 서비스는 사용자 인증, 권한없는 클라이언트의 액세스 방지 및 데이터 변경 방지를 포함한 여러 목적을 위해 공용과 개인 키를 사용하여 데이터를 암호화합니다. 인증서를 발급 받는 사용자를 제어하여 데이터 액세스를 신뢰할 수 있는 사용자를 제어할 수 있습니다. SSL 기술은 데이터 암호화와 암호 작성을 위해 다른 여러 API에 통합됩니다.

제3부 설치 및 통합 고려사항

이 섹션에서는 구성요소가 서로 맞추어지는 방법을 설명합니다. 이는 각 제품에 대한 하드웨어 및 소프트웨어 요구사항과 필요한 모든 응용 프로그램 또는 데이터베이스 제품을 나열합니다.

제10장 FirstSecure 설치 계획

FirstSecure 구성요소 제품을 설치하기 전에 다음 섹션을 읽고 필요한 하드웨어와 소프트웨어를 가지고 있는지 확인해야 합니다. FirstSecure의 최신 갱신에 대한 정보는 www.ibm.com/software/security/firstsecure에 있습니다. 제품을 설치하기 전에 웹 사이트에서 최신 갱신에 대해 확인하십시오.

FirstSecure의 구성요소 제품을 설치하고 구성하는 상세한 단계별 지침은 각 구성요소 제품의 제품 문서에서 제공됩니다.

일반적인 시스템 요구사항

이 섹션은 FirstSecure 제품의 전체적인 시스템 요구사항을 설명합니다. 각 구성요소 제품에 대한 특정 하드웨어 및 소프트웨어 요구사항에 대해 해당 구성요소 제품을 참조하십시오.

FirstSecure 구성요소를 설치하려면, 다음 서버 운영 체제 중 하나를 실행할 수 있는 하드웨어가 필요합니다.

- 서비스 팩 5가 설치된 Microsoft Windows NT 버전 4.
- AIX 버전 4.3.1 이상.
- Sun Solaris 버전 2.6 이상.

  주: Solaris의 Toolbox에서 1999년 5월 수정팩이 있는 Sun Solaris 버전 2.6이 필요합니다.

각 FirstSecure 구성요소 제품은 적어도 앞에서 언급한 운영 체제 중 하나에서 실행합니다. 각 구성요소 제품 섹션은 지원되는 운영 체제 플랫폼과 각 구성요소 제품의 기타 필수 소프트웨어를 보여줍니다. 이런 운영 체제에서 서버, 관리 콘솔 및 클라이언트 시스템이 필요합니다. 다음 섹션은 이런 요구사항에 대한 개요를 제공합니다.

서버 및 클라이언트에 대한 운영 체제 요구사항

SecureWay 제품의 운영 체제 요구사항에 대해서는 표1을 참조하십시오.

표 1. 서버 및 클라이언트에 대한 운영 체제 요구사항

운영 체제	최소 서버 레벨	최소 클라이언트 레벨
Windows NT	버전 4.0, 서비스팩 5	버전 4.0, 서비스팩 5
IBM AIX	버전 4.3.1	버전 4.3.1
Sun Solaris	버전 2.6	버전 2.6
Windows 95	N/A	모든 버전 지원됨
Windows 98	N/A	모든 버전 지원됨
Windows 3.1(Norton AntiVirus 전용)	N/A	모든 버전 지원됨
IBM OS/2(Norton AntiVirus 전용)	N/A	버전 4.0, 수정팩 6 이상

구성요소 제품 세부사항 및 요구사항

다음 섹션에서는 FirstSecure 구성요소 제품에 대한 하드웨어 및 소프트웨어 요구사항을 보여줍니다. 다음 장은 구축 블록을 상세하게 설명하고 각각에 대해 하드웨어 및 소프트웨어 요구사항을 제공합니다. 다음 장에서는 또한 각 제품의 설치 및 구성 개요와 다른 구성요소와의 통합에 대한 설명을 제공합니다.

- 63 페이지의 『제11장 Policy Director 요구사항 및 설치 고려사항』
- 65 페이지의 『제12장 SecureWay Boundary Server 요구사항 및 설치 고려사항』
- 73 페이지의 『제13장 Intrusion Immunity 요구사항 및 설치 고려사항』
- 81 페이지의 『제14장 공용 키 하부구조 요구사항 및 설치 고려사항』
- 87 페이지의 『제15장 Toolbox 설치 요구사항 및 고려사항』

제11장 Policy Director 요구사항 및 설치 고려사항

이 장에서는 Policy Director의 하드웨어 및 소프트웨어 요구사항을 나열합니다. 이는 또한 다른 FirstSecure 제품과의 통합에 대한 설치 고려사항을 제공합니다.

Policy Director 하드웨어 및 소프트웨어 요구사항

표2는 Policy Director 하드웨어 요구사항을 보여줍니다.

표 2. Policy Director의 하드웨어 요구사항

플랫폼	최소 디스크 공간	최소 메모리
Windows NT 서버: Intel 또는 Intel 호환가능한 80486 133 MHZ 이상	16 MB	64 MB
AIX 서버: AIX 4.3.1을 실행하는 하드웨어	16 MB	64 MB
Solaris 서버: Solaris 2.6을 실행하는 하드웨어	16 MB	64 MB

Policy Director 구성요소의 소프트웨어 요구사항은 다음과 같습니다.

Policy Director 서버

- Windows NT 서버 버전 4.0, 서비스팩 5
- AIX 버전 4.3.1
- Sun Solaris, 버전 2.6

NetSEAT 클라이언트

- Windows NT 서버 버전 4.0, 서비스팩 5
- Windows 95
- Windows 98

관리 콘솔

- Windows NT 워크스테이션
- Windows NT 서버 클라이언트

- AIX 버전 4.3.1 클라이언트
- Sun Solaris, 버전 2.6 클라이언트

Policy Director에서는 패키지에 포함된 기타 소프트웨어가 필요합니다. *IBM SecureWay Policy Director Up and Running*의 지시에 따라 Policy Director 전개에 필요한 소프트웨어를 설치하십시오.

Policy Director 설치 및 고려사항

www.ibm.com/software/security/policy는 Policy Director의 현재 소프트웨어에 대한 모든 갱신을 나열합니다.

Policy Director 및 Trust Authority 통합

IBM SecureWay Trust Authority는 각 사용자가 스스로 주장하는 사용자인지를 인증합니다. Trust Authority는 때때로 Lightweight Directory Access Protocol나 LDAP라고 하는 IBM SecureWay Directory의 정보를 기반으로 사용자에게 인증서를 발급합니다.

Policy Director는 다시 이런 인증서를 사용하고 각 사용자가 허용된 자원만 액세스하는지 확인하여 권한을 부여합니다. Policy Director는 그 정보를 같은 IBM SecureWay Directory에 저장합니다.

e-business에는 모든 Policy Director 허용과 모든 Trust Authority 정보가 들어 있는 사용자 정의가 하나 있습니다. SecureWay Boundary Server 정보를 IBM SecureWay Directory에도 저장하면 Policy Director는 사용자를 위해 그 정보를 관리할 수 있습니다.

제12장 SecureWay Boundary Server 요구사항 및 설치 고려사항

이 장에서는 SecureWay Boundary Server의 하드웨어 및 소프트웨어 요구사항을 나열합니다. 이는 또한 다른 SecureWay Boundary Server 제품과의 통합에 대한 설치 고려사항을 제공합니다.

SecureWay Boundary Server 하드웨어 및 소프트웨어 요구사항

SecureWay Boundary Server 구성요소 제품의 하드웨어 요구사항은 표3과 66 페이지의 표4에 있습니다.

표 3. SecureWay Boundary Server 구성요소 제품에 대한 하드웨어 요구사항

SecureWay Boundary Server 구성요소	시스템 유형	디스크 공간	메모리	기타
IBM SecureWay Firewall[1]	NT: Pentium® 133 MHz 이상 AIX: AIX 4.3.2를 지원하는 RS/6000 시스템	NT: 24 MB[2] AIX: 307MB	NT: 64MB AIX: 64MB	2개의 네트워크 인터페이스 카드
ACE/Server	NT: Pentium 166 MHz 이상 (단일 프로세서 전용) AIX: AIX 4.2를 지원하는 시스템	기본 서버 소프트웨어: 50 MB 백업 서버: 22 MB 초기 사용자 데이터베이스: 4MB 설치: 240MB	최소: 32MB	실제 저장영역 필요량은 사용자 집단에 따라 다릅니다.
SurfinGate				
서버	Pentium 233 MHz 이상	20 MB	최소: 128 MB 권장: 256 MB	

표 3. SecureWay Boundary Server 구성요소 제품에 대한 하드웨어 요구사항 (계속)

SecureWay Boundary Server 구성요소	**시스템 유형**	**디스크 공간**	**메모리**	**기타**
콘솔	Pentium 233 MHz 이상	15 MB	최소: 32 MB 권장: 64 MB	
IBM SecureWay 릴리스 2용 MIMEsweeper				
MAILsweeper	Pentium 200 MHz 이상	1 GB	64 MB	1개의 네트워크 인터페이스 카드
WEBsweeper	Pentium 400 MHz 이상	1 GB	각 동시 웹 연결에 대해 128 MB + 1 MB	1개의 네트워크 인터페이스 카드

주:

1. 더 자세한 내용에 대해서는 IBM Firewall에 포함된 문서를 참조하십시오.
2. NetScape 브라우저에 대해서도 13 MB의 디스크 공간이 필요합니다.

표 4. SecureWay Boundary Server 구성요소 제품에 대한 소프트웨어 요구사항

SecureWay Boundary Server 구성요소	**Microsoft Windows 플랫폼**		**AIX**	**Solaris**
	클라이언트	**서버**	**서버**	**서버**
IBM SecureWay Firewall	Windows 95, IPSec 클라이언트	Windows NT 서버 버전 4.0, 서비스팩 5[1]	AIX 4.3.2	사용불가
ACE/Server	Windows NT 워크스테이션 4.0, 서비스팩 2 이상	Windows NT 서버 버전 4.0, 서비스팩 5 이상	AIX 4.2	Solaris 2.5.1
SurfinGate 4.05				
서버	사용불가	Windows NT 4.0[2]	사용불가	사용불가
콘솔	Windows NT 4.0 이상[2] Windows 95, Windows 98	사용불가	사용불가	사용불가
IBM SecureWay 릴리스 2용 MIMEsweeper				
MAILsweeper	사용불가	Windows NT 4.0[3]	사용불가	사용불가

표 4. SecureWay Boundary Server 구성요소 제품에 대한 소프트웨어 요구사항 (계속)

SecureWay Boundary Server 구성요소	Microsoft Windows 플랫폼		AIX	Solaris
	클라이언트	서버	서버	서버
WEBsweeper	Windows NT 워크스테이션 4.0, 서비스팩 3 이상	Windows NT 4.0[4]	사용불가	사용불가

주:

1. 필요한 수정에 대해 Windows NT용 IBM Firewall과 함께 제공된 문서에서 확인하십시오.
2. 추가적으로
   - Microsoft Windows용 Windows 네트워크 클라이언트가 필요합니다.
   - Windows NT 워크스테이션은 지원되지 않습니다.
3. 추가적으로
   - NT 3.5.1과 Windows NT 워크스테이션은 지원되지 않습니다.
   - 다음 환경 중 하나가 필요합니다.
     - Microsoft Exchange
     - SMTP
     - cc:Mail™
     - Groupwise
     - Lotus Notes
4. MIMEsweeper 권장에 대해 71 페이지의 『MIMEsweeper 고려사항』을 참조하십시오.

SecureWay Boundary Server 구성요소 고려사항

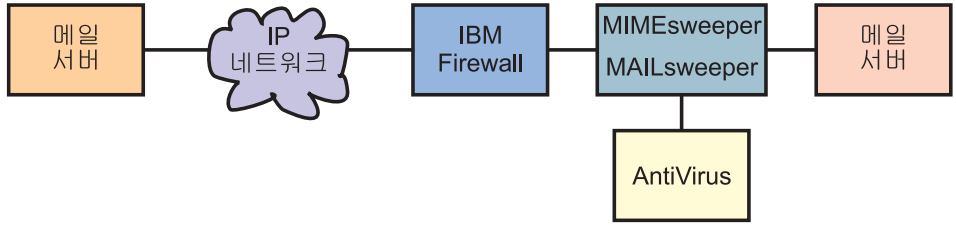
다음 섹션은 SecureWay Boundary Server 구성요소 제품의 설치 및 구성 고려사항을 설명합니다.

IBM Firewall 고려사항

IBM Firewall에 대한 고려사항은 주로 기타 SecureWay Boundary Server 제품에 관하여 트래픽 스트림에서 이를 설치하는 위치와 관련되어 있습니다.

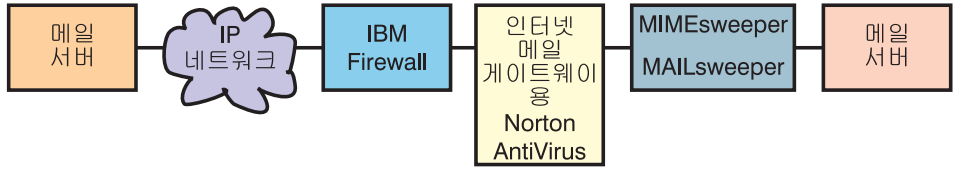
샘플 구성

IBM Firewall 및 MAILsweeper 보기 구성: IBM Firewall과 MIMEsweeper를 둘 다 설치하는 경우 이 섹션에서 설명한 구성을 사용할 수 있습니다.



- MAILsweeper는 메일 메시지 내용을 점검하는 MIMEsweeper의 일부입니다. MAILsweeper에는 antivirus 점검을 수행하는 기능이 있습니다.
- MAILsweeper는 IBM Firewall 및 보안 SMTP 서버 사이에 있습니다.
- IBM Firewall은 메일을 전달할 메일 호스트로서 MAILsweeper를 가리킵니다.
  - IBM Firewall에서는 사전에 정의된 메일 규칙은 메일 트래픽이 흐르도록 설정되어야 합니다.
- SMTP 서버도 메일을 전달할 메일 호스트로서 MAILsweeper를 가리켜야 합니다.
- MAILsweeper는 양방향으로 흐르는 전달된 메일의 내용을 점검합니다.

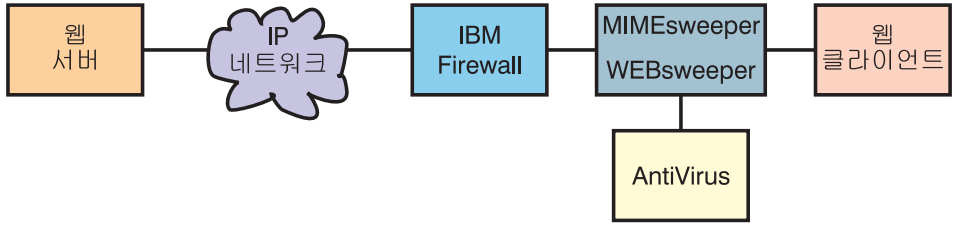
IBM Firewall, Norton AntiVirus for Internet Email Gateways 및 MIMEsweeper 샘플 구성: IBM Firewall, Norton AntiVirus for Internet Email Gateways 및 MIMEsweeper를 설치하는 경우 이 섹션에서 설명한 구성을 사용할 수 있습니다. 이 시나리오에서는 IBM Firewall, Norton AntiVirus for Internet Email Gateways 및 MAILsweeper를 하나의 체인으로 묶어 다음 다이어그램에서 설명한 것처럼 메일에서 바이러스와 내용을 점검합니다.



- Firewall은 보안 메일 서버로서 Norton AntiVirus for Internet Email Gateways를 가리킵니다. 올바른 Firewall 규칙은 이 특정 트래픽을 허용하도록 설정되어야 합니다.

- Norton AntiVirus for Internet Email Gateways는 보안 메일에 대한 메일 전송자로서 MAILsweeper를 가리키고, 메일의 목적지 아웃바운드로서 Firewall을 가리킵니다.
- MAILsweeper는 전달된 메일을 수신하고 점검합니다. 그런 다음 이는 라우팅 표나 MX 레코드 검색에 따라 올바른 서버로 메일을 전달합니다. MAILsweeper 및 Norton AntiVirus for Internet Email Gateways가 같은 시스템에 있으면, MAILsweeper의 수신 포트를 변경하여 Norton AntiVirus for Internet Email Gateways와의 충돌을 예방하십시오.

IBM Firewall 및 WEBsweeper 샘플 구성: IBM Firewall과 MIMEsweeper를 둘 다 설치하는 경우 이 섹션에서 설명한 구성을 사용할 수 있습니다.

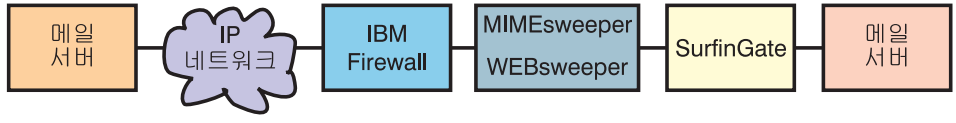


- WEBsweeper는 웹 트래픽을 점검하는 MIMEsweeper의 일부입니다. WEBsweeper에는 antivirus 점검을 수행하는 기능이 있습니다.
- WEBsweeper는 중계 프록시로서 작동합니다. 클라이언트는 WEBsweeper를 프록시로 가리킵니다. WEBsweeper는 트래픽을 Firewall 프록시로 전송하도록 설정됩니다.
- 규칙은 프록시 트래픽을 허용하도록 Firewall에서 설정되어야 합니다.
- 프록시 요청은 Firewall 배후에 있는 보안 네트워크에서만 발생할 수 있습니다.
- WEBsweeper는 HTTPS를 처리하지 않습니다. HTTPS를 사용하려면, Firewall의 문제점 및 모든 웹 트래픽 점검 확인의 문제점을 피할려면 WEBsweeper를 통과시켜야 합니다. Firewall 프록시를 직접 가리켜야 합니다. 웹 트래픽은 계속 안전하지만 WEBsweeper가 점검하지는 않습니다.

IBM Firewall 및 SurfinGate 샘플 구성: IBM Firewall과 SurfinGate를 설치하는 경우 이 섹션에서 설명한 구성을 사용할 수 있습니다.

- SurfinGate는 ActiveX 제어 및 기타 항목에 대한 웹 트래픽을 점검합니다.
- SurfinGate는 중계 웹 프록시로서 작동합니다. 클라이언트는 SurfinGate를 HTTP, FTP 및 HTTPS에 대한 프록시로서 가기킵니다. SurfinGate는 그런 다음 요청을 IBM Firewall 프록시에 전달합니다.
- 규칙은 프록시 트래픽을 허용하도록 Firewall에서 설정되어야 합니다.
- 프록시 요청은 Firewall 배후에 있는 보안 네트워크에서만 발생할 수 있습니다.

IBM Firewall, MIMEsweeper 및 SurfinGate 샘플 구성: IBM Firewall, MIMEsweeper 및 SurfinGate를 설치하는 경우 이 섹션에서 설명한 구성을 사용할 수 있습니다



- SurfinGate는 ActiveX 제어 및 기타 항목에 대한 웹 트래픽을 점검합니다. MIMEsweeper의 WEBsweeper 구성요소와는 다른 점검을 사용합니다.
- SurfinGate 및 WEBsweeper는 중계 웹 프록시로서 작동합니다. 클라이언트는 SurfinGate를 HTTP 및 FTP에 대한 프록시로서 가리킵니다. 그런 다음 SurfinGate는 요청을 WEBsweeper로 전달합니다. WEBsweeper는 요청을 IBM Firewall 프록시에 전달합니다.
- 규칙은 프록시 트래픽을 허용하도록 Firewall에서 설정되어야 합니다. 이러한 규칙들은 *Windows NT용 IBM eNetwork Firewall 버전 3.3 사용자 안내서*에서 정의됩니다.
- 프록시 요청은 Firewall 배후에 있는 보안 네트워크에서만 발생할 수 있습니다.
- WEBsweeper는 HTTPS를 처리하지 않습니다. HTTPS를 사용하는 경우 Firewall의 문제점 및 모든 웹 트래픽 점검 확인의 문제점을 피할려면 WEBsweeper를

통과시켜야 합니다. Firewall 프록시를 직접 가리켜야 합니다. 웹 트래픽은 계속 안전하지만 WEBsweeper가 점검하지는 않습니다.

MIMEsweeper 고려사항

다음은 일반적인 WEBsweeper 시스템입니다.

- Intel Pentium 400 MHz 이상
- 1GB 디스크 공간 및 128 MB RAM
- Windows NT 서버 또는 워크스테이션 버전 4.0 서버 서비스팩 3 이상
- 호스트와 도메인 이름을 포함한 TCP/IP 프로토콜
- antivirus 툴

다음은 동시 사용자를 최대 500명까지 허용할 수 있는 일반적인 고볼륨 WEBsweeper 환경입니다.

- 이중 Intel Pentium II, 450 MHz 이상
- 3GB 디스크 공간 및 256 MB RAM
- Windows NT 서버 또는 워크스테이션 버전 4.0 서버 서비스팩 3 이상
- 호스트와 도메인 이름을 포함한 TCP/IP 프로토콜
- antivirus 툴

사용자 환경이 동시 사용자를 500명 이상 지원하면 다중 WEBsweeper 서버를 사용하는 것이 바람직합니다.

제13장 Intrusion Immunity 요구사항 및 설치 고려사항

이 장에서는 Intrusion Immunity 구성요소인 Tivoli Cross-Site for Security와 Norton AntiVirus의 하드웨어와 소프트웨어 요구사항을 나열합니다.

Intrusion Immunity 하드웨어 및 소프트웨어 요구사항

다음 섹션에서는 Intrusion Immunity 구성요소 제품에 대한 설치 및 구성 문서를 설명합니다.

Tivoli Cross-Site for Security에 대한 하드웨어 및 소프트웨어 요구사항은 표5, 74 페이지의 표6 및 74 페이지의 표7에 있습니다. Norton AntiVirus 구성요소 제품에 대한 하드웨어와 소프트웨어 요구사항은 75 페이지의 표8 및 75 페이지의 표9에 있습니다.

표 5. Tivoli Cross-Site for Security 서버에 대한 하드웨어 및 소프트웨어 요구사항

서버 요구사항	
운영 체제	• AIX 4.3.2 • Windows NT 버전 4.0, 서비스팩 5 • Solaris 2.5.1 또는 2.6
Java	JDK 1.1.6 개정판 04 이상
웹 서버	Netscape Enterprise Server 3.51
데이터베이스	• IBM DB2 릴리스 5.2 • Oracle 7.3.4(또는 8.0.4 권장) • Microsoft SQL Server
디스크 공간	• Windows NT 290 MB • AIX 180 MB • Solaris 180 MB
메모리	256 MB
스왑 공간	300 MB(400 MB 권장)

표 5. Tivoli Cross-Site for Security 서버에 대한 하드웨어 및 소프트웨어 요구사항 (계속)

서버 요구사항
주: 1. Netscape Enterprise Server 3.51과 3.6은 지원되지 않습니다. 2. Tivoli Cross-Site for Security의 설치 문서에 있는 Solaris용 패치 요구사항을 참조하십시오.

표 6. Tivoli Cross-Site for Security 관리 콘솔에 대한 하드웨어 및 소프트웨어 요구사항

관리 콘솔 요구사항	
운영 체제	• Windows 95 • Windows 98 • Windows NT 버전 4.0, 서비스팩 5(166 MHz 이상의 시스템 권장) • Sun SPARC에서 실행하는 Solaris 2.5.1이나 2.6
디스크 공간	모든 플랫폼에 대해 25 MB
메모리	• Windows NT 40 MB • AIX 64 MB • Solaris 40 MB

표 7. Tivoli Cross-Site for Security 에이전트에 대한 하드웨어 및 소프트웨어 요구사항

에이전트 요구사항	
운영 체제	• Windows NT 버전 4.0, 서비스팩 5 이상 • AIX 4.3.2 • Sun SPARC에서 실행하는 Solaris 2.5.1이나 2.6
Java	Solaris에서의 JDK 1.1.6 개정판 04 이상(UNIX에서만 필요)
디스크 공간	• Windows NT에서 15 MB • AIX에서 10 MB • Solaris에서 10 MB
메모리	• Windows NT에서 32 MB • AIX에서 32 MB • Solaris에서 20 MB

표 7. Tivoli Cross-Site for Security 에이전트에 대한 하드웨어 및 소프트웨어 요구사항 (계속)

에이전트 요구사항
주: 1. Netscape Enterprise Server 3.51과 3.6은 지원되지 않습니다. 2. Tivoli Cross-Site for Security의 설치 문서에 있는 Solaris용 패치 요구사항을 참조하십시오.

표8은 Norton AntiVirus의 하드웨어 요구사항을 나열합니다.

표 8. Norton AntiVirus의 하드웨어 요구사항.

Intrusion Immunity 구성요소	**시스템 유형**	**디스크 공간**	**메모리**	**기타**
Norton AntiVirus	Intel CPU	24 MB	최소: 16 MB 권장: 32 MB	CD-ROM 드라이브
Norton AntiVirus for Internet E-mail Gateways	Pentium 133 이상	6 MB	32 MB	CD-ROM 드라이브 효율적인 메일 운영을 위해 500 MB - 5 GB

표 9. Norton AntiVirus의 소프트웨어 요구사항

Intrusion Immunity 구성요소	**Microsoft Windows 플랫폼**		**OS/2**
	클라이언트	**서버**	**클라이언트**
Norton AntiVirus[1]	Windows NT 4.0 Windows 95, Windows 98	Windows NT 4.0	OS/2 2.11 이상
주: 1. 추가적으로 TCP/IP 인터넷 연결이 Norton AntiVirus for Internet Email Gateways에 필요합니다.			

Norton AntiVirus는 AIX와 Solaris에서 사용할 수 없습니다.

Tivoli Cross-Site for Security 설치 및 고려사항

다음 그림은 e-business 네트워크에서의 일반적인 Cross-Site for Security 에이전트 및 Cross-Site for Security 관리 서버의 배치를 보여줍니다.

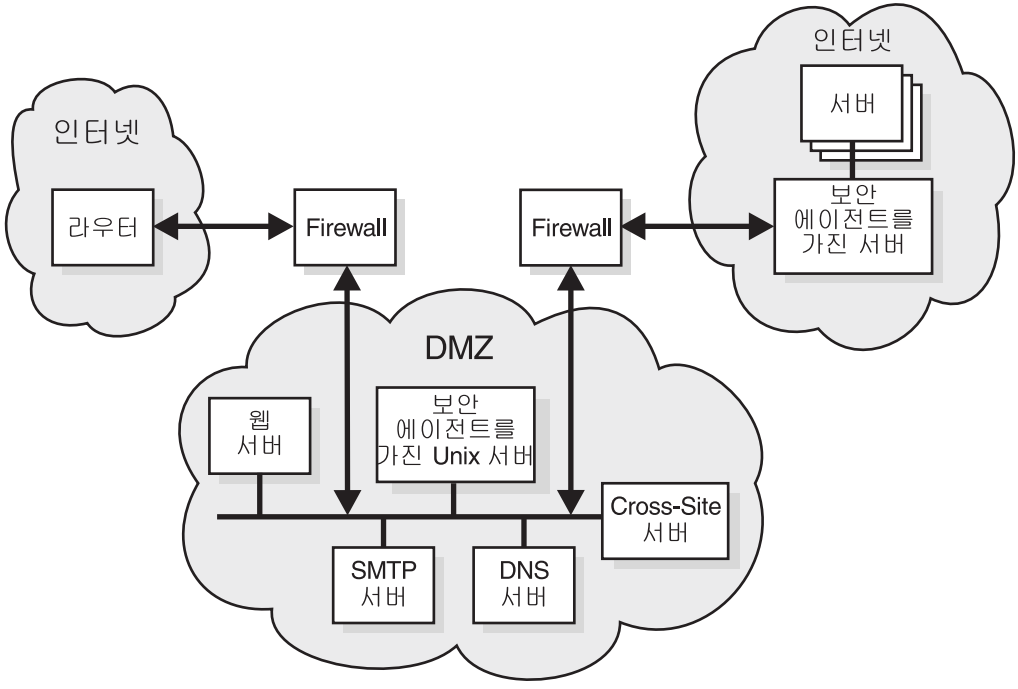


그림 11. DMZ에 Cross-Site for Security 관리 서버 설치

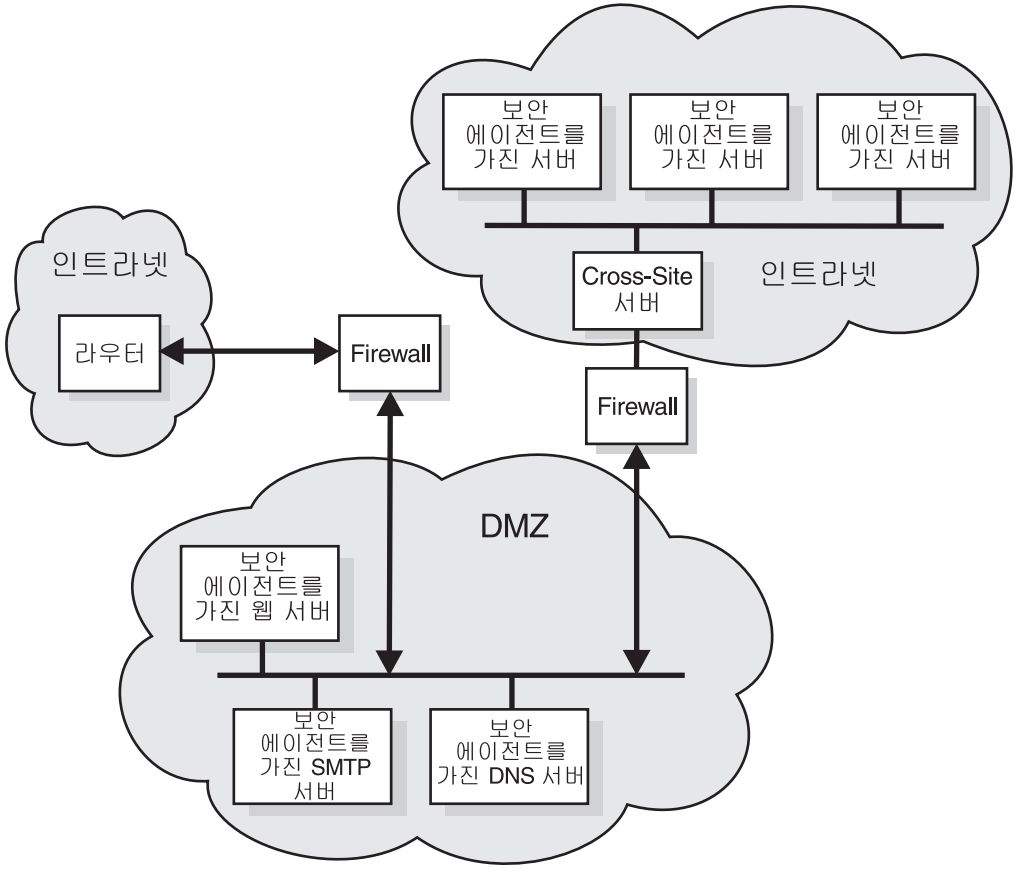


그림 12. 인트라넷에 Cross-Site for Security 관리 서버 설치

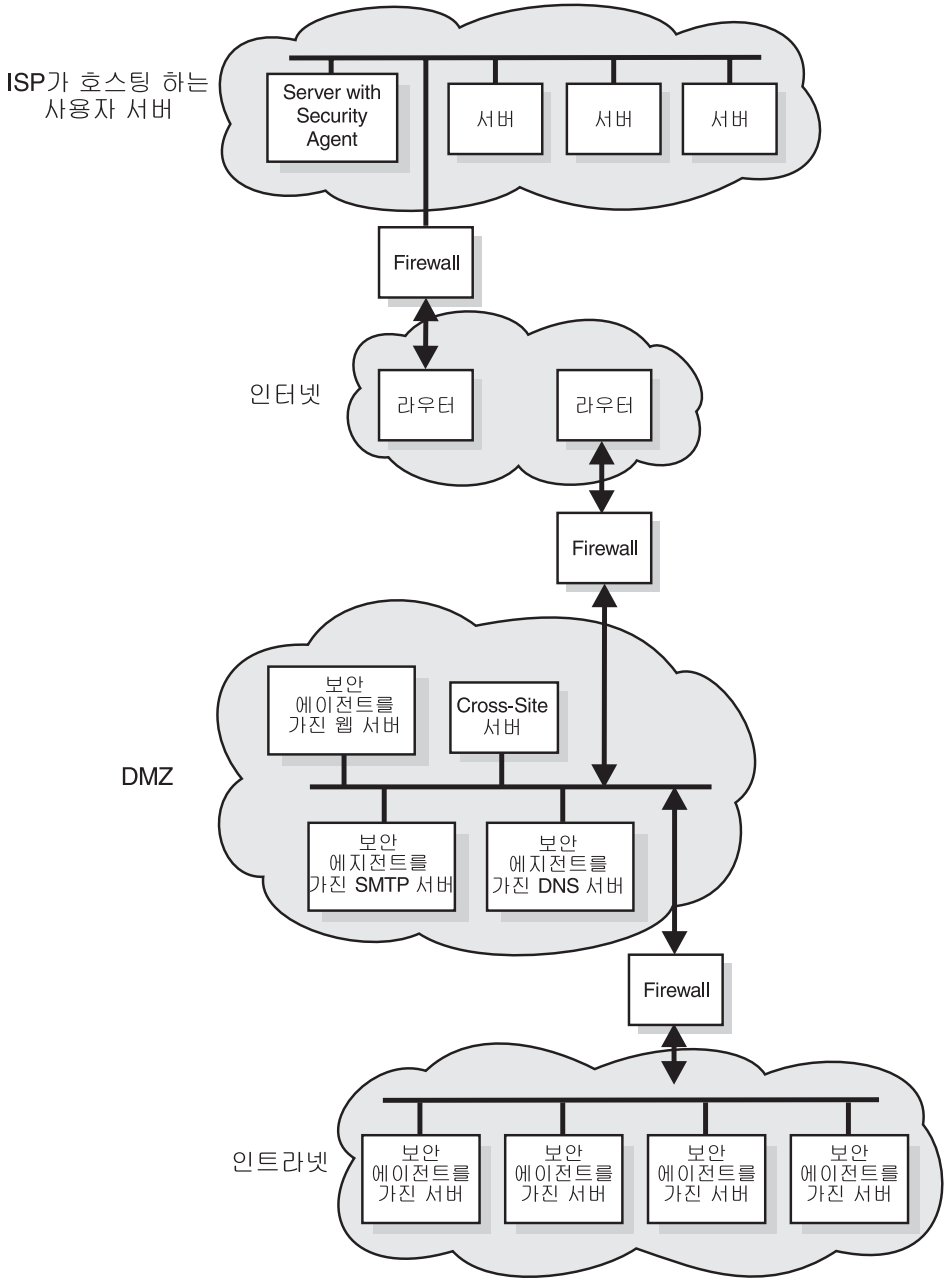


그림 13. 인터넷으로 연결된 서버를 지원하는 DMZ에서 Cross-Site for Security 관리 서버 설치

Norton AntiVirus 설치 및 고려사항

Norton AntiVirus 설치에 대한 내용은 contents.txt라는 이름의 파일에 있는데, 이는 제품 CD의 루트 디렉토리에 있습니다.

제14장 공용 키 하부구조 요구사항 및 설치 고려사항

현재 회사에서는 e-business 응용 프로그램을 안전하게 하기 위한 공용 키 하부구조가 필요하므로, FirstSecure Trust Authority에서는 공용 키 하부구조를 구현하는 두 레벨의 기능을 제공합니다.

- 디지털 인증서의 완전한 수명 관리는 다음을 제공합니다.
  - 인증을 요청, 갱신 및 철회하는 기능
  - 인증 요청을 승인하는 등록 권한
  - 디지털 인증서와 취소 목록을 작성하는 인증 기관
- 비지니스가 신뢰된 e-business 엔티티 온라인을 등록하는 향상된 등록 기능. 등록 응용 프로그램은 다음을 기본으로 하여 작성됩니다.
  - 발행되어 관리되는 인증은 중요한 e-business 응용 프로그램에 필요한 신뢰성이 있어야 하며, 등록 권한은 높은 신뢰성과 보안 요구사항을 만족하도록 구성되어야 합니다.
  - 응용 프로그램은 수동 또는 자동 승인, 유연성있는 온사이트 또는 오프사이트 인증 및 등록 정책을 신뢰할 수 있는 별도의 도메인으로 분리하는 옵션을 포함하여 다양한 등록 정책을 지원하기 위한 유연성을 제공해야 합니다.

신뢰 모델은 전자 거래의 액세스 가능성, 기밀성, 통합성 및 소유권을 보장하는데 도움을 줍니다. 디지털 암호화, 인증 및 서명을 통해 Trust Authority는 인터넷, 인트라넷 또는 VPN(virtual private network)에서 보안 e-business를 관리할 수 있게 합니다. 서명 키를 더욱 보안하기 위해 인증 기관은 암호 하드웨어에 대해 작동하도록 설계되었습니다.

Trust Authority 서버 하드웨어 및 소프트웨어 요구사항

Trust Authority 구성요소에 대한 서버 소프트웨어 요구사항은 82 페이지의 표10에 있습니다.

표 10. 공용 키 하부구조 Trust Authority 구성요소에 대한 서버 소프트웨어 및 선택적 하드웨어 요구사항

제품	주
다음 운영 체제 중 하나: • IBM AIX/6000(AIX), 버전 4.3.2 • Service Pack 5가 설치된 Microsoft Windows NT 버전 4.0	• 필수. • 모든 Trust Authority 서버 프로그램을 같은 플랫폼에 설치해야 합니다. AIX와 Windows NT 시스템을 같은 시스템 구성에서 섞을 수 없습니다.
IBM SecureWay Directory 버전 3.1.1	• 필수. Trust Authority 코드와 통합되었습니다. • Trust Authority를 설치하는 중에 Trust Authority를 설치한 것과 같은 시스템에 Directory 소프트웨어를 설치하거나 이를 원격 시스템에 설치할 수 있습니다.
IBM WebSphere Application Server 버전 2.02, Standard Edition. IBM HTTP 서버 버전 1.3.3과 Sun Java Development Kit (JDK) 1.1.7을 포함합니다.	• 필수. Trust Authority 미디어 패키지에서 제공합니다. • Trust Authority를 설치하기 전에 웹 서버 소프트웨어를 Trust Authority와 Trust Authority 서버 소프트웨어를 설치할 계획인 것과 같은 시스템에 설치해야 합니다.
유지보수 패치 9를 갖춘 IBM DB2 Universal Database Enterprise Edition 버전 5.2.	• 필수. Trust Authority 미디어 패키지에서 제공합니다. • 각 서버 구성요소마다 고유한 데이터베이스 인스턴스가 있습니다. Trust Authority를 설치하기 전에 Trust Authority 서버로 사용할 계획인 각 시스템에 DB2를 설치해야 합니다.
• IBM SecureWay 4758 PCI Cryptographic Coprocessor, 모델 001 • 유지보수 패치 1.3.0.1을 갖춘 IBM SecureWay 4758 CCA Support Program, 버전 1.3.0.0	• *선택적*이고 AIX 시스템에서만 사용할 수 있습니다. 일반 IBM 주문 채널을 통해 이 제품을 주문해야 합니다. • Trust Authority를 설치하기 전에 Trust Authority CA를 설치할 계획인 서버에 4758 하드웨어와 지원 프로그램을 설치해야 합니다. • 4758 암호화 카드는 RS/6000의 PCI 버스가 필요합니다.

83 페이지의 표11 및 84 페이지의 표12는 Trust Authority의 서버 하드웨어 요구사항을 나열합니다.

83 페이지의 표11 및 84 페이지의 표12에서:

- 소규모의 생산 환경은 매일 수 백개의 인증서를 발급합니다.
- 중간 규모의 생산 환경은 매일 수 천개의 인증서를 발급합니다.
- 대규모의 생산 환경은 매일 수 없이 많은 인증서를 발급합니다. 이는 또한 타사 CA 서비스를 다른 조직에 제공하는 시스템입니다.

Windows NT에서 Trust Authority를 실행할 계획이라면 IBM은 이를 IBM Netfinity® Server에서 설치할 것을 권합니다. 다음 표는 Trust Authority Certificate Authority를 통해 발급하려고 하는 인증서의 수를 기반으로 시스템 크기 조정 권장사항을 제공합니다.

표 11. 샘플 Windows NT 시스템 구성

시스템 유형	프로세서	디스크 공간	메모리
소규모의 생산 환경			
Netfinity 3000	1 (450 MHz, Pentium II)	2 드라이브(9.1 GB)	256 MB
Netfinity 5000	2 (450 MHz, Pentium II)	2 드라이브(9.1 GB)	512 MB
중간 규모의 생산 환경			
Netfinity 3000	1 (500 MHz, Pentium III)	4 드라이브(18.2 GB)	768 MB
Netfinity 5000	2 (500 MHz, Pentium III)	4 드라이브(9.1 GB)	1 GB
대규모의 생산 환경			
Netfinity 5500	2 (450 MHz, Pentium III)	4 드라이브(9.1 GB 고속)	1 GB
Netfinity 5500	4 (500 MHz, 1024K L2 캐시가 있는 Pentium III Xeon with)	4 드라이브(9.1 GB 고속)	1 GB
Netfinity 7000	2 (500 MHz, 512K L2 캐시가 있는 Pentium III)	4 드라이브(9.1 GB 고속)	1 GB
Netfinity 7000	4 (500 MHz, 1024K L2 캐시가 있는 Pentium III Xeon with)	4 드라이브(18.2 GB)	2 GB

AIX에서 Trust Authority를 실행할 계획이라면 이를 IBM RISC System/6000® 시스템에 설치해야 합니다. 다음 표는 Trust Authority Certificate Authority를 통해 발급하려고 하는 인증서의 수를 기반으로 시스템 크기 조정 권장사항을 제공합

니다.

표 12. 샘플 AIX 시스템 하드웨어 구성

시스템 유형	프로세서	디스크 공간	메모리
소규모의 생산 환경			
F40	2 (233 MHz)	2 드라이브(9.1 GB, Ultra 2 Fast Wide)	512 MB
중간 규모의 생산 환경			
F40	2 (233 MHz)	3 드라이브(9.1 GB, Ultra 2 Fast Wide)	1 GB
대규모의 생산 환경			
F50	4 (332 MHz)	5 드라이브(9.1 GB Ultra 2 Fast Wide 하나와 9.1 GB SSA 4개)	2 GB
H50	4 (332 MHz)	5 드라이브(9.1 GB Ultra 2 Fast Wide 하나와 9.1 GB SSA 4개)	2 GB
R50	6 (200 MHz)	2 드라이브(9.1 GB Ultra 2 Fast Wide)	1 GB
R50	8 (200 MHz)	5 드라이브(9.1 GB Ultra 2 Fast Wide 하나와 9.1 GB SSA가 4개인 7133 SSA 랙)	2 GB

Trust Authority 클라이언트 하드웨어 및 소프트웨어 요구사항

IBM은 브라우저 등록 양식을 사용하고 Trust Authority 클라이언트 응용 프로그램을 실행하기 위해 다음과 같은 워크스테이션 구성을 권합니다.

- 다음 물리적 시스템 설정:
  - 최소한 32 MB 메모리의 166 MHz Intel 486 프로세서(최소한 64 MB 메모리의 200 MHz Intel Pentium 프로세서를 선호함)
  - 그래픽 카드
  - VGA 비디오 디스플레이 이상
  - 마우스 또는 마우스 호환 가능 지시 장치
- 다음 운영 체제 중 하나:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT, 버전 4.0
- 다음 웹 브라우저 중 하나:
  - Netscape Navigator 또는 Netscape Communicator, 버전 3.0 이상

– Java를 사용할 수 있는 Microsoft Internet Explorer, 버전 4.0 이상.

IBM KeyWorks Toolkit 및 IBM SecureWay Trust Authority 상호작용

IBM KeyWorks Toolkit을 IBM SecureWay Trust Authority와 같은 서버에 설치하지 마십시오.

제15장 Toolbox 설치 요구사항 및 고려사항

FirstSecure Toolbox은 e-business에서 보안 응용 프로그램을 개발할 수 있도록 도와 주는 API 세트입니다.

- 권한 부여 서비스
- 인증서 및 관리 서비스
- 디렉토리 서비스
- SSL(Secure Sockets Layer) 프로토콜 서비스
- KeyWorks 암호 및 신뢰 관리 서비스
  - IBM Key Recovery Service Provider 1.1.3.0 API. IBM Key Recovery Service Provider를 통해 암호화된 정보를 복구할 수 있습니다.
  - IBM Key Recovery Server 1.1.3.0. IBM Key Recovery Server 1.1.3.0은 권한 부여된 요청으로 키를 사용할 수 없거나 유실 또는 훼손된 경우 암호화된 정보를 복구할 수 있는 응용 프로그램입니다.

    이런 두 툴킷은 응용 프로그램이 중요한 보안 서비스뿐만 아니라 보안 제공자가 툴킷에 플러그인하기 위해 사용할 수 있는 표준 인터페이스를 호출할 때 사용하는 표준 인터페이스를 제공합니다. 표준 인터페이스는 CDSA(Common Data Security Architecture)를 기반으로 합니다. 이런 툴킷은 Windows NT, Solaris 및 AIX에서 사용할 수 있습니다.

Toolbox 하드웨어 및 소프트웨어 요구사항

Toolbox의 하드웨어 요구사항은 표13에 있습니다.

표 13. Toolbox의 하드웨어 요구사항

플랫폼	디스크 공간	메모리
버전 4.0, 서비스팩 5	2 - 4 GB	64 MB
AIX 4.3.2	9.1 GB	1 GB
1999년 5월 Fix Pak이 있는 Sun Solaris, 버전 2.6	4.2 GB	128 MB

표 14. Toolbox 구성요소 제품에 대한 하드웨어 요구사항

툴킷	시스템 유형	디스크 공간	메모리
IBM KeyWorks Toolkit	다음 환경에서 수행되는 제품을 지원하는 하드웨어: Windows NT 버전 4.0, 서비스팩 5 이상 Windows 95 AIX 4.2 이상 Sun Solaris	50 MB	32 MB
IBM Key Recovery Service Provider	다음 환경에서 수행되는 제품을 지원하는 하드웨어: Windows NT 버전 4.0, 서비스팩 5 이상 Windows 95 AIX 4.2 이상 Sun Solaris	50 MB	32 MB

Toolbox 구성요소 제품에 대한 소프트웨어 요구사항은 다음 표에서 표시됩니다.

표 15. Toolbox 구성요소 제품에 대한 소프트웨어 요구사항

Toolbox 구성요소	**Microsoft Windows 플랫폼**		**AIX**	**Solaris**
	클라이언트	**서버**	**서버**	**서버**
IBM KeyWorks Toolkit	Windows NT 버전 4.0, 서비스 팩 5 이상	Windows NT 버전 4.0, 서비스 팩 5 이상 Windows 95	AIX 4.2 이상[1]	Sun Solaris
IBM Key Recovery Service Provider	Windows NT 버전 4.0, 서비스 팩 5 이상[2] Windows 95	Windows NT 버전 4.0, 서비스 팩 5 이상	AIX 4.2 이상	Sun Solaris

주:

1. AIX 클라이언트도 지원됩니다.
2. 추가적으로 IBM KeyWorks Toolkit도 필요합니다.

IBM KeyWorks Toolkit 1.1

IBM KeyWorks Toolkit 1.1은 서로 다른 작업 환경에서 암호 및 기타 보안 기능에 액세스하는 개방형이며 확장가능하고 표준인 방법을 응용 프로그램 개발자에게 제공합니다.

IBM KeyWorks Toolkit는 응용 프로그램이 서비스 제공자 추가 모듈이 툴킷과 인터페이스하는 데 사용할 수 있는 표준 인터페이스뿐만 아니라 응용 프로그램이 중요한 암호, 신뢰 및 보안 서비스를 호출하는 데 사용할 수 있는 표준 인터페이스(API)를 제공합니다. 이러한 표준 인터페이스는 CDSA(Common Data Security Architecture)를 기본으로 하며, 이는 초기에 Intel™사가 개발하고 IBM에 의해 KeyWorks Toolkit으로 확장된 Open Group의 표준입니다. 표준 인터페이스를 사용하는 경우 다음을 수행할 수 있습니다.

- 회사는 보안 서비스를 사용하는 응용 프로그램을 변경하지 않고도 요구사항에 가장 적합한 암호 및 신뢰 설치를 선택할 수 있습니다.
- 응용 프로그램 및 미들웨어 프로그래머의 생산성이 향상됩니다.

IBM KeyWorks Toolkit은 응용 프로그램과 미들웨어 사이에 클래스와 암호화 기능 및 서비스 제공자로서 격리 계층을 제공합니다. 툴킷에는 프레임워크와 서비스 제공자 플러그인 모듈이 들어 있습니다.

응용 프로그램의 경우, 프레임워크는 Intel사의 CDSA에서 기능이 풍부한 CSSM(Common Security Services Manager)을 제공합니다. IBM은 키 복구 기능을 추가하여 CSSM API를 확장했습니다. IBM KeyWorks Toolkit을 사용하면 응용 프로그램이 다음을 수행할 수 있습니다.

- 정보 암호화 및 암호 해독
- 여러 목적으로 디지탈 서명 검증
- 디렉토리에서 인증 및 인증 취소 리스트 검색
- 키 복구 및 암호화 백업을 위한 키 복구 필드 작성
- 사용자 지시하에 시스템 디자이너와 프로그래머가 설정한 기준을 근거로 인증의 신뢰 여부를 결정

일반적으로 엔터프라이즈 또는 OEM은 IBM KeyWorks Toolkit 및 IBM Key Recovery Service Provider 툴킷을 CSSM 프레임워크에서 CSSM API의 사용을 허용하는 방식으로 응용 프로그램 및 미들웨어와 통합합니다. 이 통합의 제품은 운영 환경(들)에서 배포되는 서버 및 클라이언트용 런타임 응용 프로그램 및 미들웨어의 세트입니다. FirstSecure의 다른 요소들은 시간이 지남에 따라 모든 암호화 서비스 및 신뢰 정책에 대한 IBM KeyWorks Toolkit에 따라 달라집니다.

IBM KeyWorks Toolkit을 사용하는 통합자는 미들웨어와 프레임워크뿐만 아니라 암호화 디자인 및 프로그래밍에 대해 상당한 경험을 가진 시스템 엔지니어와 프로그래머를 직원으로 고용하거나 이런 경험이 있는 통합자 또는 OEM과 계약을 해야 합니다.

서비스 제공자의 경우 프레임워크는 Open Group의 CDSA인 표준 SPI(Service Provider Interface)를 제공합니다. IBM은 키 복구 기능으로 SPI를 향상시켰습니다.

IBM KeyWorks Toolkit(SDK)에는 개방형 표준 및 특허 공용 키 인증을 지원하는 플러그인 서비스 제공자 모듈이 들어 있습니다. 이러한 모듈에는 PKCS#11, RSA 데이터 보안의 BSAFE 암호화 기능, X.509V3 인증, Entrust 및 Verisign

의 신뢰 정책 및 LDAP(Lightweight Directory Access Protocol)이 포함됩니다. 프레임워크는 각각의 독립적인 서비스 제공자 모듈이 제공하는 암호화되고 신뢰되는 보안 기능들을 매끄럽게 통합합니다.

IBM KeyWorks Toolkit은 다음과 같은 중요 관리 기능들을 제공할 수 있습니다.

- KeyWorks 지원 프로세스에서 중요한 과정을 생략하지 않도록 보호
- 서비스 제공자 플러그인 모듈이 사용하기 전에 변경되지 않도록 검증
- 프레임워크를 통해서만 서비스 제공자 플러그인 모듈 사용
- 국가 고유 및 회사 고유의 암호 및 신뢰 정책 사용 지원

IBM KeyWorks Toolkit은 다음과 같은 이득을 제공합니다.

- 응용 프로그램 및 미들웨어를 다시 작성하지 않고도 서비스 제공자 모듈을 변경하거나 대체할 수 있습니다.
- 하드웨어 암호화 및 디지탈 특성에 대한 원활한 지원을 제공합니다.
- LDAP 디렉토리 및 DSA 서명 표준을 지원합니다.
- 특별한 인증 권한을 사용하지 않아도 됩니다.

IBM KeyWorks Toolkit에 대한 자세한 내용은 *IBM KeyWorks Toolkit Developer's Guide*에 있습니다.

IBM KeyWorks Toolkit 및 IBM SecureWay Trust Authority 상호작용

IBM KeyWorks Toolkit을 IBM SecureWay Trust Authority와 같은 서버에 설치하지 마십시오.

IBM Key Recovery Service Provider Toolkit 1.1

툴킷 형식으로 제공되는 IBM Key Recovery Service Provider 1.1.3.0 은 IBM KeyWorks Toolkit이 제공하는 표준 기능을 사용하는 서비스 제공자 모듈입니다. IBM Key Recovery Service Provider를 사용하면 개인 키를 수집하고 보관한 다음 암호의 약점이 될 수 있는 포인트를 작성하지 않고도 암호화되어 저장 및 전송된 정보를 복구할 수 있습니다.

IBM Key Recovery Service Provider는 IBM KeyWorks Toolkit이 제공하는 표준 기능을 사용하므로, 키 복구 기능은 다른 암호 제공자, 여러 인증 권한의 표준 인증, Verisign 및 Entrust의 신뢰 정책 및 LDAP이 액세스할 수 있는 디렉토리에서 사용될 수 있습니다. IBM Key Recovery Service Provider는 이들간의 통신과 연관된 세션 키를 근거로 키 복구 정보를 작성합니다.

IBM Key Recovery Service Provider에 대한 자세한 내용은 FirstSecure 문서 팩에서 제공하는 *Key Recovery Server Installation and Usage Guide*에 있습니다.

제16장 FirstSecure에서 제공하는 문서

FirstSecure에 들어있는 각 구성요소 제품은 자신의 문서를 제공합니다. 이 장에서는 FirstSecure 구성요소 제품과 함께 들어있는 문서에 대한 정보를 제공합니다.

SecureWay FirstSecure, SecureWay Policy Director 및 SecureWay Boundary Server에 대해 미디어 팩과 문서를 사용할 수 있습니다. 미디어 팩에는 구성요소 제품을 설치할 때 사용하는 제품 CD가 있으며 이런 CD에는 온라인 문서 중 일부가 있습니다. 문서 팩에는 구성요소 제품을 제공하는 것에 대한 하드카피 문서가 들어 있습니다. 103 페이지의 『FirstSecure 문서 팩』은 문서 팩의 내용을 나열합니다.

Policy Director

다음 문서는 Policy Director 구성요소 제품과 함께 제공됩니다.

IBM SecureWay Policy Director Up and Running
: IBM SecureWay Policy Director를 설치하고 구성하는 방법을 알려줍니다.

IBM SecureWay Policy Director Administration Guide
: IBM SecureWay Policy Director를 관리하는 방법을 알려줍니다. 이 책은 PDF 형식으로 제공됩니다.

IBM SecureWay Policy Director Programming Guide and Reference
: IBM SecureWay Policy Director에 대해 프로그램을 작성하는 방법을 알려줍니다. 이 책은 PDF 형식으로 제공됩니다.

제품 **readme**
: 이 정보는 웹의 www.ibm.com/software/security/policy에서 얻을 수 있습니다.

SecureWay Boundary Server

다음 책은 SecureWay Boundary Server 구성요소 제품, 그 요구사항과 상호작용을 설명합니다.

IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running
SecureWay Boundary Server 구성요소 제품을 설명하는 하드카피 책.

다음 섹션에서는 SecureWay Boundary Server 구성요소 제품과 함께 제공된 문서에 대해 설명합니다.

IBM SecureWay Firewall

모든 IBM Firewall 문서는 소프트카피로 제공됩니다. IBM Firewall에서는 다음 문서를 제공합니다.

IBM SecureWay Firewall for AIX Setup and Installation
AIX용 IBM SecureWay Firewall 설치 및 설정 지침.

IBM SecureWay Firewall for Windows NT Setup and Installation
Windows NT용 IBM SecureWay Firewall 설치 및 설정 지침.

IBM SecureWay Firewall for AIX User's Guide
Windows NT용 IBM SecureWay Firewall 설치 및 설정 지침.

IBM SecureWay Firewall for Windows NT User's Guide
Windows NT용 IBM Firewall 사용에 대한 정보.

IBM SecureWay Firewall for Windows NT Reference
Windows NT용 IBM Firewall 사용에 대한 참조 자료가 들어 있습니다.

IBM SecureWay Firewall for AIX Reference
AIX용 IBM Firewall 사용에 대한 참조 자료가 들어 있습니다.

IBM SecureWay Firewall Problem Determination Guide for Windows NT and AIX 문제 판별에 대한 지침이 들어 있습니다.

IBM SecureWay Firewall VPN Client User's Guide
VPN(virtual private network) 설정 및 사용 방법을 알려줍니다.

MIMEsweeper

MIMEsweeper에는 다음 문서가 들어 있습니다.

MIMEsweeper Administrator's Guide

릴리스 정보 섹션에 들어있으며, 다음에는 계획 및 설치 정보를 포함하여 관리자를 위한 정보가 들어 있습니다.

이 문서는 제품 CD에서 HTML 형식으로 제공됩니다. 웹 브라우저에서는 \DOC\MANUAL.HTM 파일을 보고 이것을 온라인으로 볼 수 있습니다.

MIMEsweeper Release Notes

문서를 온라인으로 보기 위한 지침과 설치 내용을 포함하여 갱신된 문서가 들어 있습니다.

이 문서는 제품 CD에서 HTML 형식으로 제공됩니다. 웹 브라우저에서는 \DOC\RELNOTES.HTM 파일을 보면 온라인으로 볼 수 있습니다.

MIMEsweeper Configuration Editor Help

MIMEsweeper 구성 파일 편집에 대한 정보가 들어 있습니다.

이 문서는 제품 CD에서 HTML 형식으로 제공됩니다.

SurfinGate

SurfinGate에는 다음과 같은 소프트카피 문서가 들어 있습니다.

SurfinGate Installation Guide

Windows NT에서 SurfinGate 4.05 구성요소를 설치하고 구성하는 것에 대한 정보. *SurfinGate 설치 안내서*의 PDF 버전은 \docs\install.pdf 파일의 제품 CD에 들어 있습니다.

SurfinGate User Guide

SurfinGate 계획 및 사용에 대한 정보. *SurfinGate User Guide*의 PDF 버전은 제품 CD에 있는 \docs\manual.pdf 파일에서 제공됩니다.

SurfinGate 4.05 for Windows NT Release Notes

시스템 요구사항과 제품 제한을 포함하는 SurfinGate 4.05에 대한 정보. *SurfinGate 4.05 for Windows NT Release Notes*의 PDF 버전은 제품 CD에 있는 \docs\relnotes.pdf 파일에서 제공됩니다.

SurfinGate for Windows NT/UNIX Solaris Release Notes, Appendix A

SurfinGate에 대한 변경사항을 설명하는 온라인 문서. 이 문서는 \docs\rnappen.pdf 파일의 제품 CD에 있습니다.

Intrusion Immunity

다음 섹션에서는 Intrusion Immunity 구성요소 제품과 함께 제공된 문서에 대해 설명합니다.

Tivoli Cross-Site for Security

Tivoli Cross-Site for Security, 버전 1.1에는 .pdf 형식으로 된 다음 문서가 들어 있습니다.

Tivoli Cross-Site for Security Installation

이 문서는 설치의 상세한 요구사항을 제공하고 설치 단계를 안내해 줍니다.

Tivoli Cross-Site for Security User's Guide

이 문서는 제품 개요, 콘솔 사용 및 작업 수행 지침, 명령 행 인터페이스와 같은 참조 정보, 구성 파일 및 용어해설을 제공합니다. 이 문서는 제품 CD에 있습니다.

Norton AntiVirus

Norton AntiVirus에는 FirstSecure에서 제공되는 구성요소에 대한 다음 문서가 들어 있습니다 contents.txt 파일을 제외한 모든 문서들은 Norton AntiVirus CD에서 PDF 형식으로 전달됩니다. contents.txt 파일은 제품 CD에서 ASCII 파일입니다.

Norton AntiVirus Solution Release 3.04 CD의 문서 목차

\contents.txt라고 하는 Norton AntiVirus Solution Release 3.04 CD 파일은 CD에 들어 있는 모든 문서를 나열합니다.

관리 솔루션:

Norton AntiVirus Solution Implementation Guide

제품 CD의 \docs\admin\navimp.pdf를 참조하십시오.

Norton AntiVirus Command-Line Scanner

제품 CD의 \docs\navc\navcugd.pdf를 참조하십시오.

비상 복구 디스크 작성

제품 CD의 \navc\readme.txt를 참조하십시오.

서버 솔루션:

Norton AntiVirus for Windows NT Server Administrator's Guide

제품 CD의 \docs\admin\navnts50.pdf를 참조하십시오.

Norton AntiVirus for NetWare User's Guide

제품 CD의 \docs\NAVNLM\NVN4.pdf를 참조하십시오.

Norton AntiVirus for Lotus Notes Installation Guide

제품 CD의 \docs\NAVNOTES\NAVNOTES.pdf를 참조하십시오.

Norton AntiVirus for Lotus Notes Installation Guide

제품 CD의 \docs\NAVNOTES\NAVNOTES.pdf를 참조하십시오.

Norton AntiVirus for OS/2 Lotus Notes Installation Guide

제품 CD의 \docs\NOTESOS2\NOTESOS2.pdf를 참조하십시오.

Norton AntiVirus for Microsoft Exchange Installation Guide

제품 CD의 \docs\NAVXCHNG\NAVXCHNG.pdf를 참조하십시오.

게이트웨이 솔루션:

Norton AntiVirus for Internet Email Gateway User's Guide

제품 CD의 \docs\navieg\navieg.pdf를 참조하십시오.

Norton AntiVirus for Firewalls Administrator's Guide

제품 CD의 \docs\navfw\navfw.pdf를 참조하십시오.

데스크탑 솔루션:

Norton AntiVirus User's Guide for Windows 3.1/DOS

제품 CD의 \docs\navwks\nav4dusr.pdf를 참조하십시오.

Norton AntiVirus Reference Guide for Windows 3.1/DOS
제품 CD의 \docs\navwks\nav4dref.pdf를 참조하십시오.

Norton AntiVirus for Windows 95/98 User's Guide
제품 CD의 \docs\navwks\nav98usr.pdf를 참조하십시오.

Norton AntiVirus for Windows 95/98 Reference Guide
제품 CD의 \docs\navwks\nav98ref.pdf를 참조하십시오.

Norton AntiVirus for Windows NT User's Guide
제품 CD의 \docs\navwks\nav5nusr.pdf를 참조하십시오.

Norton AntiVirus for Windows NT Reference Guide
제품 CD의 \docs\navwks\nav5nref.pdf를 참조하십시오.

Norton AntiVirus v4.0 User's Guide for Windows NT
제품 CD의 \docs\351\navntugd.pdf를 참조하십시오.

Norton AntiVirus v4.0 Reference Guide for Windows NT
제품 CD의 \docs\351\navntref.pdf를 참조하십시오.

Norton AntiVirus User's Guide for OS/2
제품 CD의 \docs\navos2\navos2ug.pdf를 참조하십시오.

Norton AntiVirus Distribution Guide for OS/2
제품 CD의 \docs\navos2\navos2dg.pdf를 참조하십시오.

Norton AntiVirus for Macintosh User's Guide
제품 CD의 \docs\navmac\navmac.pdf를 참조하십시오.

Norton AntiVirus Solution Release 3.04 CD 백서: CD는 또한 \sarc 디렉토리에 백서를 포함합니다. 각 백서는 .pdf 형식으로 되어 있습니다.

Norton AntiVirus Solution Release 3.04 CD 비디오: CD는 또한 비디오를 포함합니다. 비디오를 보려면 미디어 플레이어나 .AVI 파일을 재생할 수 있는 다른 프로그램이 있어야 합니다. 비디오는 다음 파일에 있습니다.

SARC \sarc\sarc.avi

바이러스 정보
\sarc\aboutvir.avi

Norton AntiVirus: 안내서

\navtour\guided\demo32.exe

Norton AntiVirus의 경보에 응답하는 방법

\navtour\alert\demo32.exe

Norton System Center 안내

\nsctour\setup.exe

또는 CD에서 직접 안내를 받으려면

\nsctour\demo32.exe

\ncstour\readme.txt 파일에서의 안내에 대한 더 자세한 정보

Trust Authority

IBM SecureWay Trust Authority 제품 문서는 *Trust Authority 문서* CD-ROM에서 PDF(Portable Document Format)와 HTML 형식으로 사용할 수 있습니다. 대부분의 정보는 Trust Authority에서 지원하는 언어로 변환되었습니다. 선택한 언어로 출판물을 액세스하는 방법에 대해서는 제품 *Readme* 파일을 참조하십시오. *Readme* 파일의 최신 버전은 http://www.ibm.com/software/security/trust/library의 IBM SecureWay Trust Authority 웹 사이트의 라이브러리 페이지에서 항상 얻을 수 있습니다.

Trust Authority 라이브러리에는 다음과 같은 문서가 들어 있습니다.

IBM SecureWay Trust Authority Up and Running

이 책은 제품의 개요입니다. 이는 제품 요구사항을 나열하고 설치 절차를 포함하며 각 제품 구성요소에 대해 사용할 수 있는 온라인 도움말을 액세스하는 방법에 대한 정보를 제공합니다. *문서* CD-ROM에서 얻을 수 있는 것 외에 이 책은 인쇄판으로 제품과 함께 배포됩니다.

IBM SecureWay Trust Authority System Administration Guide

이 책에는 Trust Authority 시스템을 관리하는 것에 대한 일반 정보가 들어 있습니다. 여기에는 서버 시작 및 중지, 암호 변경, 인증 기관 관리, 감사 수행 및 데이터 무결성 확인 절차가 들어 있습니다.

IBM SecureWay Trust Authority Configuration Guide

이 책에는 설정 마법사를 사용하여 Trust Authority 시스템을 구성하는 방법에 대한 정보가 들어 있습니다. 마법사의 온라인 도움말을 보면서 이 안내서의 HTML 버전을 액세스할 수 있습니다.

IBM SecureWay Trust Authority Registration Authority Desktop Guide

이 책에는 RA 데스크탑를 사용하여 인증서 수명 전반에 걸쳐 인증서를 관리하는 방법에 대한 정보가 들어 있습니다. 데스크탑의 온라인 도움말을 보면서 이 안내서의 HTML 버전을 액세스할 수 있습니다.

IBM SecureWay Trust Authority User's Guide

이 책에는 인증서를 얻는 방법에 대한 정보가 들어 있습니다. 이는 브라우저, 서버 및 장치에 대한 인증서를 요청하는 Trust Authority 등록 양식 사용 절차를 제공합니다. 이는 또한 사용자에게 PKIX 인증서를 사전에 등록하는 방법과 Trust Authority 클라이언트를 사용하여 PKIX 인증서를 저장하고 관리하는 방법을 보여줍니다. 클라이언트의 온라인 도움말을 보면서 이 안내서의 HTML 버전을 액세스할 수 있습니다.

Toolbox

다음 섹션에서는 Toolbox 구성요소 제품과 함께 제공된 문서에 대해 설명합니다.

Toolbox API

모든 Toolbox 문서는 www.ibm.com/software/security/firstsecure/library의 웹 사이트에서 얻을 수 있습니다. 다음 문서가 포함됩니다.

IBM SecureWay Secure Sockets Layer Toolkit Programming Guide and Reference

API와 iKeyman의 개요를 제공합니다. 각 API와 그 구문 및 사용법을 정의합니다.

IBM SecureWay Directory Client SDK Programming Reference

다양한 LDAP 샘플 클라이언트 프로그램과 LDAP 서버에 대한 응용 프로그램 액세스를 제공하는 LDAP 클라이언트 라이브러리를 포함합니다. C와 Java를 지원합니다.

IBM SecureWay Policy Director Programming Guide and Reference
각 API와 그 구문 및 사용법을 정의합니다.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Installation Guide 설치 지침과 요구사항을 제공합니다.

IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms Programming Guide and Reference
PKIX로도 알려진 IBM SecureWay X.509 Public Key Infrastructure for Multiplatforms를 사용하여 응용 프로그램을 개발하는 프로그래머에게 정보를 제공합니다. 제품 개요, 별도의 PKIX 구성요소에 대한 프로그램 작성 지침 및 PKIX API의 설명을 포함합니다.

IBM KeyWorks Toolkit

IBM KeyWorks Toolkit과 함께 제공되는 모든 문서는 제품 CD에서 PDF 형식으로 되어있는 온라인입니다. 문서는 다음과 같습니다.

IBM KeyWorks Toolkit Developer's Guide
툴킷의 개요를 제공합니다. 또한 툴킷을 응용 프로그램과 통합하는 방법에 대해 설명하고 보기 응용 프로그램이 들어 있습니다.

IBM KeyWorks Toolkit Application Programming Interface (API) Specification
프레임워크 및 서비스 제공자 모듈이 제공하는 보안 서비스에 액세스하기 위해 응용 프로그램 개발자가 사용하는 인터페이스를 정의합니다.

IBM KeyWorks Toolkit Service Provider Module Structure & Administration
모든 툴킷 서비스 제공자 모듈에 공통적인 기능에 대해 설명합니다. 이 문서는 서비스 제공자 모듈을 빌드하기 위해 각각의 서비스 제공자 인터페이스 스펙과 결합되어 사용되어야 합니다.

IBM KeyWorks Toolkit Cryptographic Service Provider Interface Specification
툴킷을 통해 액세스할 수 있도록 암호 서비스 제공자 모듈이 따라야 하는 인터페이스를 정의합니다.

IBM Key Recovery Service Provider Interface (KRSPI) Specification
툴킷을 통해 액세스할 수 있도록 Key Recovery Service Provider 모듈이 따라야 하는 인터페이스를 정의합니다.

IBM KeyWorks Toolkit Trust Policy Interface Specification

인증 권한, 인증 발행자 및 방침 결정 응용 프로그램 개발자와 같은 정책 결정자가 모델 또는 응용 프로그램 고유의 방침으로 툴킷을 확장하기 위해 준수해야 하는 인터페이스를 정의합니다.

IBM KeyWorks Toolkit Certificate Library Interface (CLI) Specification

인증 라이브러리 개발자가 여러 툴킷 응용 프로그램 및 신뢰 방침 모듈에 형식 고유의 인증 조작 서비스를 제공하기 위해 준수해야 하는 인터페이스를 정의합니다.

IBM KeyWorks Toolkit Data Storage Library Interface (DLI) Specification

라이브러리 개발자가 형식 고유의 또는 형식과는 관계없는 영구적인 인증 저장영역을 제공하기 위해 준수해야 하는 인터페이스를 정의합니다.

IBM Key Recovery Service Provider

다음 문서는 제품 CD에서 PDF 형식으로 IBM Key Recovery Service Provider와 함께 제공됩니다.

IBM Key Recovery Service Provider Key Recovery Server Installation and Usage Guide

키 복구 개념, 조직의 키 복구 솔루션 설정 지침 및 IBM 키 복구 서버 설치, 구성 및 조작 절차에 대한 내용을 제공합니다.

보안 redbook

IBM ITSO(International Technical Support Organization)에서 만든 다음 redbook은 보안 관련 제품과 프로세스를 다룹니다. www.us.ibm.com/redbooks에서 얻을 수 있습니다.

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

문서 팩

다음 문서 팩은 IBM SecureWay FirstSecure에서 사용할 수 있습니다.

FirstSecure 문서 팩

FirstSecure 문서 팩에는 다음 책이 있습니다.

- FirstSecure 라이센스 정보
- *IBM SecureWay FirstSecure Planning and Integration*
- *IBM SecureWay Policy Director Up and Running*
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*
- *IBM SecureWay Trust Authority Up and Running*
- *Tivoli Cross-Site for Security Installation*

Policy Director 문서 팩

Policy Director 문서 팩에는 다음 책이 있습니다.

- Policy Director 라이센스 정보
- *IBM SecureWay Policy Director Up and Running*

SecureWay Boundary Server 문서 팩

SecureWay Boundary Server 문서 팩에는 다음 책이 있습니다.

- SecureWay Boundary Server 라이센스 정보
- *IBM SecureWay Boundary Server for Windows NT and AIX: Up and Running*

제4부 부록 및 끝머리

부록. 주의사항

이 정보는 미국에서 제공하는 제품과 서비스용으로 개발되었으며, IBM은 이 책에서 설명하는 제품, 서비스 또는 기능을 다른 나라에서 제공하지 않을 수도 있습니다. 현재 해당 국가에서 사용할 수 있는 제품 및 서비스에 대한 정보는 현지 IBM 영업부에 문의하십시오. IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 의미는 아닙니다. 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 검증은사용자의 책임입니다.

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

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

2바이트(DBCS) 정보와 관련된 사용권에 대해서는 현지 IBM 지적 재산권부에 문의하거나 다음 주소로 서면 문의하십시오.

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 조항은 해당 내용이 지역법에 위배되는 영국 및 기타 국가에는 적용되지 않을 수도 있습니다. IBM은 상업성 또는 특정 목적에 대한 타당성에 대한 보증을 포함하여(단, 이에 국한되지는 않음) 명시적이거나 암시적인 어떤 종류의 보증도 제공하지 않고『현상대로』이 책을 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 암시적 보증의 거부를 허용하지 않으므로, 이 조항이 사용자에게 적용되지 않을 수도 있습니다.

이 책에는 기술상의 오류나 인쇄상의 오류가 있을 수 있습니다. 이 책에 들어 있는 정보는 정기적으로 변경되며 이러한 변경사항은 이 책의 개정판에 수록됩니다. IBM은 언제든지 통보없이 이 책에 기술된 제품 및/또는 프로그램을 변경하거나 개선할 수 있습니다.

이 책에 언급된 타사 웹 사이트는 단지 사용자의 편의를 위한 것이며 이들 웹 사이트를 후원한다는 의미는 아닙니다. 이들 웹 사이트의 자료는 이 제품을 구성하는 자료의 일부가 아니며 이들 웹 사이트의 사용으로 인해 발생하는 문제는 사용자의 책임입니다.

IBM은 독자가 제공한 정보를 적절한 방식으로 사용하거나 배포할 수 있으며제공한 독자는 이에 대한 책임을 지지 않습니다.

(i)독립적으로 작성된 프로그램과 다른 프로그램(이 프로그램을 포함한)간의 정보 교환과 (ii)교환된 정보의 상호 사용을 목적으로 이 프로그램에 대한 정보를 필요로 하는 사용권자는 다음 주소로 문의하십시오.

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

일부 경우 사용료 지불을 비롯하여 적절한 조건을 준수하면 이러한 정보를 사용할 수 있습니다.

이 책에 기술된 사용권 프로그램 및 사용가능한 모든 사용권 자료는 IBM이 IBM 고객 계약, IBM 국제 프로그램 사용권 계약 또는 그와 동등한 계약 하에 제공한 것입니다.

여기에 포함된 모든 성능 데이터는 통제된 환경에서 결정된 데이터입니다. 따라서 다른 운영 환경에서 도출된 결과와 크게 다를 수 있습니다. 일부 측정은 개발 수준의 시스템에서 수행 되었으며 일반적으로 가용한 시스템에서 측정하는 경우와 동일한 결과가 나온다는 아무런 보증이 없습니다. 더우기 일부 측정은 보외법을 사용하였으므로 실제 결과는 다를 수 있습니다. 본 문서의 사용자는 자신의 특정한 환경에 대해 적용가능한 데이터를 입증해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급자, 공표된 내용 또는 기타 공개적으로 가용한 소스를 통해 얻을 수 있습니다. IBM은 이러한 제품을 점검하지 않았으며 성능의 정확성, 호환성 또는 비IBM 제품과 관련된 기타 소송에 대해 보증하지 않습니다. 비IBM 제품의 성능에 관한 사항은 해당 제품의 공급자에게 문의하십시오.

IBM의 향후 방침 또는 계획에 대한 모든 공고는 통지 없이 변경 또는 철회될 수 있으며 여기서는 단지 목표와 방향을 제시하는 것입니다.

IBM이 제시한 소비자 가격은 현재의 가격이며 통지 없이 변경될 수 있습니다. 판매 가격은 다를 수 있습니다.

이 정보는 계획용으로만 사용됩니다. 여기에 있는 정보는 설명한 제품을 사용할 수 있게 되기 전에 변경될 수 있습니다.

등록상표

다음 용어는 미국 또는 기타 국가에서 IBM 사의 등록상표입니다.

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

Intel 및 Pentium은 미국 및 기타 국가에서 Intel사의 등록상표입니다.

Java 및 모든 Java 기본 등록상표와 로고는 미국 및 기타 국가에서 Sun Microsystems사의 등록상표입니다.

Lotus, Lotus Notes, Domino 및 cc:Mail은 미국이나 다른 나라에서 Lotus Development Corporation의 상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 및 기타 국가에서 Microsoft 사의 등록상표입니다.

Tivoli는 미국 및 기타 국가에서 Tivoli Systems사의 등록상표입니다.

UNIX는 미국과 다른 나라에서 X/Open Company Limited를 통해서만 라이센스를 받을 수 있는 등록상표입니다.

기타 회사, 제품 및 서비스 이름은 타사의 등록상표나 서비스 상표입니다.

용어

이 용어해설은 이 책에서 사용하는 새롭거나 생소한 용어 또는 흥미있는 용어 및 축약어를 정의합니다. 여기에는 다음 책에서 나온 용어와 정의가 들어 있습니다.

- The IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- The American National Standard Dictionary for Information Systems, ANSI X3.172–1990, American National Standards Institute (ANSI), 1990.
- The Answers to Frequently Asked Questions, Version 3.0, California: RSA Data Security, Inc., 1996.

가

감사 추적(audit trail). 논리 경로의 형식으로 일련의 이벤트를 링크하는 데이터입니다. 감사 추적은 트랜잭션이나 주어진 활동의 히스토리를 추적할 때 사용됩니다. 예를 들어, 이는 고객 계정에서 활동을 추적할 수 있습니다.

게이트웨이(gateway). 비호환 네트워크나 응용 프로그램이 서로 통신할 수 있도록 하는 시스템입니다.

공용 키(public key). 다른 모든 사람들이 사용할 수 있는 공용/개인 키 쌍의 키입니다. 이를 통해 사용자는 트랜잭션을 키 소유자에게 보내거나 디지털 서명을 확인할 수 있습니다. 공용 키로 암호화된 데이터는 해당 개인 키를 통해서만 해독될 수 있습니다. 공용/개인 키 쌍을 *참조하십시오.*

공용/개인 키 쌍(public/private key pair). 공용/개인 키 쌍은 키 쌍 암호와 개념의 일부입니다(키 관리 문제를 해결하기 위해 Diffie와 Hellman이 1976년에 도입함). 그 개념에서 각 사람은 공용 키와 개인 키라고 하는 키 쌍을 확보합니다. 각 사람의 개인 키는 비밀로 유지되는 반면 공용 키는 모두 사용할 수 있도록 공개됩니다. 송신자와 수신자는 비밀 정보를 공유할 필요가 없습니다. 모든 통신에는 공용 키만 관련되어 있으며 개인 키는 전송되거나 공유되는 경우가 없습니다. 더 이상 일부 통신 채널이 틈이나 밀고로부터 안전하다고 신뢰할 필요가 없습니다. 공용 키는 신뢰할 수 있는 디렉토리와 같은 신뢰할 수 있는(인증된) 방식으로 그 사용자에 관련되어 있다는 것만이 유일한 요구사항입니다. 누구든지 공용 정보를 사용하여 기밀 정보를 전송할 수 있습니다. 그러나, 메시지는 의도한 수신인이 소유한 개인 키에 의해서만 해독될 수 있습니다. 더군다나, 키 쌍 암호화는 개인(암호화)뿐만 아니라 인증(디지털 서명)에 대해서도 사용할 수 있습니다.

구현 서비스(Implementation Services). IBM에서 제공하는 사이트에서의 설치 지원입니다.

국제 자원 위치 지정자(Universal Resource Locator). 웹 오브젝트의 경로가 서비스 이름, 조직 이름, 경로 및 파일 이름으로 시작하는 월드 와이드 웹 통신에 사용되는 명명 규칙입니다. 예를 들어, http://www.ibm.com/software/security/firstsecure 입니다.

권한 부여(Authorization). 사용자가 수행할 수 있는 활동의 유형을 결정하는 프로세스입니다. 일반적으로, 권한 부여는 인증 다음에 발생합니다.

나

내용 필터링(Content filtering). 전송이 특정 내용 표준을 만족시키는지를 결정하기 위해 내용을 읽는 전송을 숨깁니다.

네트워크 주소 필터링(network address filtering). 수신인이나 송신인의 승인 가능성을 확인하기 위해 들어오거나 나가는 전자 우편의 주소를 확인하는 프로세스입니다.

다

디먼(daemon). AIX에서 요청을 처리하기 위해 상주해 있는 프로그램입니다.

디지털 인증서(Digital certificate). 신뢰할 수 있는 제3자가 개인이나 엔티티에 발급한 전자 인증서입니다. 인증서에는 인증하는 엔티티에 대한 정보가 들어 있습니다.

마

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

매크로 폭탄(macro bomb). 원하지 않는 결과를 초래하기 위해 다른 사용자에게 전송된 저장된 명령 순서입니다.

모빌 코드(mobile code). 여러 장소를 자주 이동하면서 다이얼 업, LAN 또는 무선 등이 여러 유형의 네트워크 연결을 사용하는 사용자에 의해 휴대용 컴퓨터에서 수행되는 작업에 속하는 것입니다.

바

비-부인(non-repudiation). 문서의 서명자가 서명한 사실을 거짓으로 거부하지 못하도록 하는 디지털 개인 키의 사용입니다.

사

사건(incident). Tivoli Cross-Site for Security에서 시스템에 대한 침입일 수 있는 의심가는 활동입니다.

서버(server). (1) 네트워크에서 다른 스테이션에 기능을 제공하는 데이터 스테이션입니다. 예를 들어, 파일 서버를 들 수 있습니다. (2) TCP/IP에서 다른 사이트에 있는 시스템의 요청을 처리하는 네트워크에 있는 시스템은 클라이언트/서버라고 합니다.

셀 디렉토리 서비스(Cell directory service). DCE(Distributed Computing Environment) 셀에 있는 자원에 대한 정보 데이터베이스를 관리하는 DCE의 구성요소입니다.

셀(cell). DCE에서 보통 공동의 목적을 가지고 모여 있는 사용자 그룹, 시스템 및 자원으로서 보안, 관리 및 명명 경계를 공유합니다. 셀은 보통 공동의 목적과 셀 외부에 있는 사용자, 시스템 및 자원보다는 서로에 대해 더 높은 수준의 신뢰를 공유하는 사용자, 시스템 및 자원으로 구성됩니다.

스팸(spam). 종종 다수의 수신인에게 전송되는 불필요한 이메일입니다.

아

암호화(encrypt). 해당 해독 코드를 알고 있는 사람만이 해독을 통해 원래 정보를 얻을 수 있도록 정보를 뒤섞어 놓는 것입니다.

애플릿(Applet). Java로 작성되고 Netscape Navigator와 같은 Java 호환 브라우저에서 실행하는 컴퓨터 프로그램입니다. Java 애플릿이라고도 합니다.

액세스 제어 목록 정의(access control list). 권한을 부여 받은 사용자가 특정 자원을 사용하는 경우 그 범위를 제한하는 메커니즘입니다.

액세스 제어(Access control). 컴퓨터 보안에서 권한을 부여 받은 사용자가 허용된 방법으로만 컴퓨터 시스템의 자원을 액세스할 수 있도록 보장하는 프로세스입니다.

에이전트(agent). Tivoli Cross-Site for Security에서 패킷을 포착하고 서로 다른 네트워크 계층에서의 이상을 확인하며 설정된 연결과 통계의 상태를 계속 추적하는 스마트 IP 패킷 모니터입니다.

엑스트라넷(extranet). 비슷한 기술을 사용하는 것으로 인터넷에서 파생되었습니다. 회사는 웹 출판, 전자 상거래, 메시징 및 그룹웨어를 여러 고객, 파트너 및 내부 직원 그룹에 적용하기 시작했습니다.

오브젝트 요청 브로커(object request broker). 객체 지향 프로그래밍에서 오브젝트가 투명하게 요청과 응답을 교환할 수 있게 하여 중간의 역할을 수행하는 소프트웨어입니다.

원격 절차 호출(remote procedure call). (1) 클라이언트가 서버의 절차 호출의 실행을 요청할 때 사용하는 기능입니다. 이 기능에는 절차의 라이브러리와 외부 데이터 표현이 포함됩니다. (2) 다른 노드에 위치한 서비스 제공자에 대한 클라이언트 요청입니다.

웜(worm). 아무런 피해도 입히지 않는 컴퓨터 바이러스입니다.

웹 브라우저(Web browser). 데스크탑 PC에서 실행하고 월드 와이드 웹이나 로컬 페이지를 찾아볼 수 있게 하는 클라이언트 소프트웨어입니다. 이는 웹과 인터넷에서 사용할 수 있는 하이퍼미디어 자료의 대규모 컬렉션을 전세계적으로 액세스할 수 있게 하는 검색 툴입니다. 예로는 Netscape Navigator와 Microsoft Internet Explorer가 있습니다. 서버도 *참조하십시오*.

웹 서버(Web server). 정보 자원을 요청하는 브라우저 프로그램에 응답하는 서버 프로그램입니다.

웹 오브젝트(Web object). 웹 브라우저를 통해 사용할 수 있는 데이터입니다. 웹 오브젝트는 웹 페이지, 웹 페이지의 일부, 파일, 이미지, 디렉토리, CGI 프로그램 또는 Java 애플릿일 수 있습니다.

웹 응용 프로그램(Web application). 월드 와이드 웹을 통해 액세스하도록 설계된 응용 프로그램입니다.

응용 프로그램 인터페이스(application program interface). 고급 언어로 작성된 응용 프로그램에서 특정 기능을 사용할 수 있도록 하는 기능적 인터페이스입니다.

이름 공간(namespace). 디렉토리에 관련되어 있으면서 사용자가 액세스할 수 있는 이름의 외부 구조입니다.

인증 기관(certificate authority). 조직의 보안 정책을 따르고 인증서의 형식으로 된 보안 전자 ID를 할당할 책임이 있는 엔티티, 소프트웨어 응용 프로그램 또는 개인입니다. 인증 기관은 인증서를 발급하고 갱신하며 다시 호출하는 요청을 처리합니다.

인증(authentication). 통신하는 당사자의 ID를 확실하게 판별하는 프로세스입니다.

인터넷(Internet). 컴퓨터 간에 전자 통신을 제공하는 세계 전반에 걸친 네트워크 컬렉션입니다. 이를 사용하여 네트워크는 전자 우편이나 웹 브라우저와 같은 소프트웨어 장치를 통해 통신할 수 있습니다. 예를 들어, 하나의 네트워크로 연결한 일부 대학들은 다른 비슷한 네트워크와 링크하여 인터넷을 형성합니다.

인트라넷(intranet). 보통 Firewall 뒤에 상주하는 엔터프라이즈의 네트워크입니다. 이는 비슷한 기술을 사용하는

인터넷에서 파생되었습니다. 기술적으로, 인트라넷은 단지 인터넷을 확장한 것일뿐입니다. HTML(정보를 그래픽으로 표현하기 위한 언어)과 HTTP(인터넷에서 하이퍼텍스트 파일을 이동시키는 프로토콜)는 일부 공통점입니다.

자

저장소(vault). 저장소는 암호화를 사용하여 시스템 관리자 및 기타 저장소의 소유자와 같이 권한을 부여 받지 않은 사람이 정보를 폭로하지 못하도록 보호합니다. 이는 또한 디지털 서명을 사용하여 함부로 변경하지 못하도록 보호하고 디지털 인증서를 사용하여 알 수 없는 그룹과 통신하지 않도록 보호합니다. 이는 암호화, 서명 및 인증서를 사용하여 정보를 안전하게 다른 저장소로 전송하기도 합니다.

전자 상거래(e-commerce). 비지니스 간 트랜잭션을 관리하는 것입니다. 인터넷을 통한 물건과 서비스의 매매(고객, 공급업자, 공급업체 및 기타 등등과)가 이루어집니다. 이는 e-business의 1차 요소입니다.

차

채널(Channel). 신호를 전송하는 경로입니다.

카

클라이언트(Client). (1) 서버의 공유 서비스를 수신하는 기능적 단위입니다. (2) 다른 컴퓨터나 프로그램의 서비스를 요청하는 컴퓨터나 프로그램입니다.

타

텔넷(telnet). 인터넷 프로토콜 그룹에서 원격 터미널 연결 서비스를 제공하는 프로토콜입니다. 이를 통해 호스트 하나의 사용자는 원격 호스트에 로그온하고 그 호스트의 터미널 사용자에 직접 접속되어 있는 것처럼 상호작용할 수 있습니다.

통합된 개발 환경(integrated development environment). 응용 프로그램을 작성하고 중단점과 함께 실행하며 프로그램 오류에 대한 진단 도움말을 수신할 수 있게 하는 응용 프로그램 개발용 프로그램입니다.

파

프록시 서버(proxy server). 액세스를 요청하는 컴퓨터(A)와 액세스되는 컴퓨터(B)간의 중간 역할을 합니다. 그러므로, 일반 사용자가 컴퓨터의 자원을 요청하면 이 요청을 프록시 서버로 보내집니다. 프록시 서버는 요청하고 컴퓨터 B에서 응답을 받은 후 응답을 일반 사용자에게 보냅니다. 프록시 서버는 Firewall에서 월드 와이드 웹 자원을 액세스할 때 유용합니다.

프린시펄(principal). DCE에서 DCE 보안을 통해 다른 엔티티와 안전하게 통신할 수 있는 엔티티입니다. 프린시펄은 사용자, 서버 또는 컴퓨터일 수 있습니다.

플러그인(plug-in). 웹 브라우저의 일부로 사용할 수 있는 프로그램입니다.

하

하트비트(heartbeat). 활동을 확인하기 위한 프로그램과 관리 프로그램간의 통신입니다. 프로그램은 아직도 해당 작업을 수행하면서 활성화되어 있음을 관리 프로그램에 알립니다.

해커(hacker). 적절한 권한 부여 없이 컴퓨터나 시스템을 액세스하려고 하는 사람입니다. 해커는 보통 허용 없이 자원을 사용하려고 합니다.

회선 레벨 게이트웨이(Circuit-level gateway). Firewall에서 클라이언트의 요청을 Firewall을 통해 의도한 서버로 경로 재지정하는 프록시 서버입니다.

A

ACL. Access Control List(액세스 제어 목록).

ActiveX. Microsoft 프로그래밍에서 객체 지향 기술 및 용어의 세트입니다.

Apache 서버(Apache server). 자유롭게 사용할 수 있는 웹 서버 소프트웨어 세트입니다.

API. Application programming interface(응용 프로그램 인터페이스).

B

Bloodhound. Norton AntiVirus에서 바이러스를 추적하는 구성요소입니다.

D

DCE. Distributed Computing Environment(분산 처리 환경).

DCE(Distributed Computing Environment). 분산 처리 환경. 서로 다른 처리 환경에서 분산 응용 프로그램의 작성, 사용 및 유지보수를 지원하는 서비스와 툴입니다.

E

e-business. 네트워크와 컴퓨터를 통해 비지니스 트랜잭션을 관리하는 것입니다. 여기에는 물건 및 서비스의 매매가 포함됩니다. 여기서는 또한 디지털 통신을 통한 자금의 전송이 이루어집니다.

F

Firewall. 두 개 이상의 네트워크 간에 경계를 이루는 시스템이나 시스템 조합입니다.

FTP(File Transfer Protocol). 컴퓨터 간에 파일을 전송할 때 사용할 수 있는 인터넷 클라이언트/서버 프로토콜입니다.

I

IDE. Integrated development environment(통합된 개발 환경).

IntraVerse 서버. IntraVerse에서 IntraVerse 서버 소프트웨어가 들어 있고 NetSEAT 클라이언트 소프트웨어에서 실행 중인 모든 호스트 시스템과 통신할 수 있는 네트워크의 시스템입니다. IntraVerse 서버는 제품의 관련 프로그램을 실행하는 시스템이나 시스템 조합을 의미합니다.

IPSec. IETF에서 개발한 Internet Protocol Security(인터넷 프로토콜 보안) 표준입니다. IPSec는 인증, 통합성, 액세스 제어 및 기밀성의 조합을 융통성 있게 지원하는 암호 보안 서비스를 제공하기 위해 설계된 네트워크 계층 프로토콜입니다. 그 강력한 인증 기능으로 이는 여러 VPN 제품 공급업체에서 인터넷을 통한 보안 점-대-점 연결을 설정하는 프로토콜로 채택되었습니다.

ISV. Independent Software Vendor(독립 소프트웨어 공급업체).

J

Java. Sun Microsystems에서 개발했으며 네트워크를 인식하면서 그 어떤 프랫폼에도 해당하지 않는 컴퓨터 기술 세트입니다. Java 환경은 Java OS, 다양한 플랫폼에 대한 가상 시스템, 객체 지향 Java 프로그래밍 언어 및 여러 클래스 라이브러리로 구성됩니다.

JavaScript. Java와 비슷하면서 Netscape 브라우저에서 사용하기 위해 Netscape에서 개발한 스크립팅 언어입니다.

K

Kerberos. 컴퓨터를 요청하는 서비스를 인증하는 보안 메소드입니다. Kerberos는 MIT(Massachusetts Institute of Technology)의 Athena Project에서 개발되었습니다. 그리스 신화에 따르면, Kerberos는 Hades의 문을 지키는 머리가 3개인 개입니다. Kerberos는 사용자가 인증 프로세서에서 암호화된 티켓을 요청하고 이 티켓을 사용하여 서버에서 특정 서비스를 요청할 수 있게 합니다. 사용자 암호는 네트워크를 통과할 필요가 없습니다.

L

LDAP. Lightweight Directory Access Protocol.

LDAP(Lightweight Directory Access Protocol). IBM SecureWay Directory에서 LDAP는 중앙에서 저장, 갱신, 검색 및 교환할 수 있도록 디렉토리 정보를 유지보수하는 방법을 제공합니다.

M

MPEG. 영화와 애니메이션을 디지털 양식으로 압축하고 저장하기 위해 MPEG(Moving Pictures Experts Group)에 의해 개발되는 표준입니다.

O

OEM. Original equipment manufacturer(원래 장치 제조업체).

R

RPC. DCE에서 원격 절차 호출입니다.

S

SecurID 토큰(SecurID token). Security Dynamics의 ACE/Server 인증 메소드는 에는 사용자 ID와 SecurID 토큰이 있습니다. 원격으로 로그인하면 SecurID 토큰에서 암호를 받습니다. 암호는 60초마다 변하며 일회용입니다. 개방된 네트워크를 통해 누군가가 암호를 가로채도 그 암호를 사용할 수 없게 됩니다.

socks 서버(socks server). Firewall으로 통해 비보안 네트워크에 있는 서버 응용 프로그램에 보안 단방향 연결을 제공하는 회선 레벨의 게이트웨이입니다.

SOCKS 프로토콜(SOCKS protocol). 보안 네트워크에 있는 응용 프로그램이 socks 서버를 통해 Firewall을 거쳐 통신할 수 있게 하는 프로토콜입니다.

SSL(Secure Sockets Layer). (1) 가능한 한 일반 사용자에게 투명한 내장된 보안 서비스가 있는 IETF 표준 통신 프로토콜입니다. 이는 디지털 방식으로 안전한 통신 채널을 제공합니다. (2) SSL-사용 서버는 보통 다른 포트에서 표준 HTTP 요청이 아닌 SSL 연결 요청을 승인합니다. SSL은 핸드쉐이크가 한 번만 일어나야 하는 경우에 세션을 작성합니다. 핸드쉐이크가 완료된 후 통신은 암호화됩니다. 메시지 통합성 확인은 SSL 세션이 만기될 때까지 수행됩니다.

T

TCP/IP. (Transmission Control Protocol/Internet Protocol).

TCP/IP(Transmission Control Protocol/Internet Protocol). 로컬과 광역 네트워크에 대한 피어간 연결성 기능을 지원하는 통신 프로토콜 세트입니다.

U

URL. Universal Resource Locator(국제 자원 위치 지정자).

V

VPN. Virtual Private Network.

VPN(virtual private network). 원격으로 연결하기 위해 전화선 대신 인터넷을 사용하는 개인 데이터 네트워크입니다. 사용자는 통신 회사 대신 ISP(Internet Service Provider)를 통해 사내 네트워크 자원을 액세스하므로 조직은 원격 액세스 비용을 상당히 줄일 수 있습니다. VPN은 또한 데이터 교환의 보안을 향상시키기도 합니다. 전형적인 Firewall 기술에서 메시지 내용은 암호화될 수 있지만 소스와 대상 주소는 암호화할 수 없습니다. VPN 기술에서 사용자는 전체 정보 패킷(내용 및 헤더)이 암호화되고 캡슐화되는 터널 연결을 설정할 수 있습니다.

X

X.509. 보안 인터넷 네트워크에서 널리 채택되고 디지털로 서명된 PKI 인증서의 보안 관리와 분배를 지원하기 위해 설계된 인증서 표준입니다. X.509 인증서는 신뢰할 수 있는 제 3 그룹에 의해 디지털로 서명된 공용 키의 분배에 관련된 절차를 조정하는 데이터 구조를 정의합니다.

색인

R

S

T

U

V

W

X

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: IBM SecureWay FirstSecure
계획 및 통합
버전 2

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: CT7EHKO

Printed in Singapore

CT7EHKO