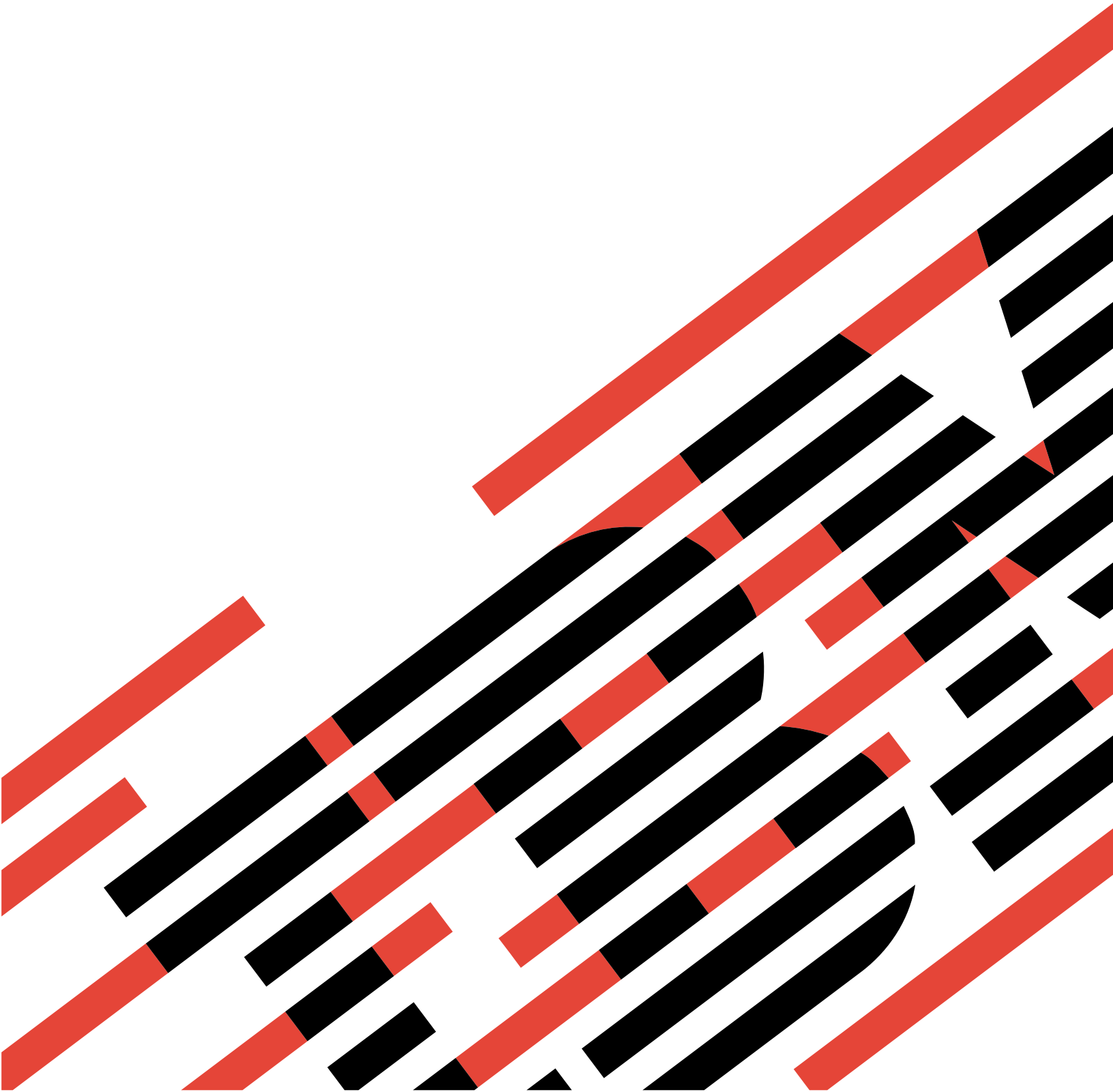
IBM

eserver

iSeries

IBM SecureWay: iSeries 400® 및 인터넷



IBM

@server

iSeries

IBM SecureWay: iSeries 400® 및 인터넷

목차

제 1 부 IBM SecureWay: iSeries 및 인터넷

LAN을 통한 인터넷 액세스는 네트워크의 변화 과정에 있어서 하나의 주요 단계이며, 이를 위해서는 사용자의 보안 요구사항을 재평가하는 것이 필요합니다. 다행스럽게도 iSeries 400에는 잠재적인 인터넷 보안의 허점과 침입자에 대비하여 강력한 방어를 구축할 수 있는 통합 소프트웨어 솔루션과 보안 구조가 있습니다. 이러한 iSeries 보안 오퍼링을 적절히 사용할 경우 고객, 직원 및 협력업체 모두 보안이 제공되는 안전한 환경에서 업무에 필요한 정보를 구할 수 있습니다.

본문의 설명을 통해 이미 널리 알려진 위험 요소와 이러한 위험 요소들이 인터넷 및 e-비즈니스 목표와 어떻게 연관되어 있는지를 알 수 있습니다. 또한 이 위험 요소들을 처리하기 위해 iSeries에서 제공하는 여러 가지 보안 옵션을 사용할 때의 이점과 각각을 비교 평가하는 방법에 관해서도 알 수 있습니다. 마지막으로, 본 정보를 사용하여 귀사의 업무 목적에 맞는 네트워크 보안 계획을 개발함으로써 확실한 보안 정책을 구현할 수 있습니다.

시스템과 자원 보호에 사용할 수 있는 인터넷 보안 위험 요소와 iSeries 보안 솔루션에 대해 자세히 알려면 다음 정보를 읽어보십시오.

- **V5R1의 새로운 사항**
  V5R1 iSeries 인터넷 보안 오퍼링에 관한 변경사항과 추가사항을 알 수 있습니다.
- **이 주제 인쇄**
  이 주제를 Adobe Acrobat 버전으로 액세스하고 인쇄할 수 있습니다.
- **iSeries 및 인터넷 보안**
  귀하가 사용할 수 있는 e-비즈니스 및 iSeries 보안 오퍼링과 관련하여 iSeries 보안의 장점을 이해할 수 있습니다.
- **인터넷 보안 계획**
  인터넷과 e-비즈니스 보안 요구에 관해 설명하는 보안 정책의 작성 방법을 알 수 있습니다.
- **기본 인터넷 준비를 위한 iSeries 시스템 보안 레벨**
  인터넷에 연결하기 전에 완료해야 할 시스템 보안 레벨에 대해 알 수 있습니다.
- **네트워크 보안 옵션**
  내부 자원을 보호하기 위해 사용해야 할 네트워크 레벨 보안 수단에 대해 알 수 있습니다.
- **어플리케이션 보안 옵션**
  위험 관리에 사용되는 여러 가지 인터넷 어플리케이션, 서비스 및 수단에서 공통적으로 발생할 수 있는 인터넷 보안 위험 요소에 관해 알 수 있습니다.
- **전송 보안 옵션**
  인터넷과 같이 신뢰할 수 없는 네트워크를 통해 자료가 지날 때 자료를 보호하기 위

해 구현할 수 있는 보안 수단에 대해 알 수 있습니다. 보안 소켓층(SSL), Client Access Express 및 VPN(가상 사설망) 연결을 사용하기 위한 보안 수단에 관해 자세히 알 수 있습니다.

- **iSeries 인터넷 보안 옵션**
  인터넷 사용과 e-비즈니스 계획을 기초로 시스템과 자원을 보호하는 오퍼링을 선택할 때 도움을 주는 iSeries 보안 옵션에 관해 자세한 설명을 제공합니다.

주: 보안과 인터넷 관련 용어에 익숙하지 않은 사용자께서는 본 자료와 함께 일반적인 보안 전문 용어를 검토하십시오.

제 1 장 V5R1의 새로운 사항

V5R1에는 iSeries 400의 보안 오퍼링에 대해 향상 및 추가된 많은 기능들이 있습니다. 다음 리스트는 몇 가지 중요한 보안 확장 기능을 정리한 것입니다.

- **디지털 인증 관리자(DCM) 확장 기능**
  DCM을 사용하여 오브젝트를 디지털로 서명함으로써 무결성을 유지하고, 오브젝트의 생성 증거를 제공하는 데 사용할 인증서를 작성 및 관리할 수 있습니다. 또한 오브젝트의 원본 여부를 확인함에 있어서 오브젝트의 자료가 변경되지 않은 것임을 보장하기 위해 사용자 본인이나 다른 사람들이 서명된 오브젝트의 서명을 인증하는 서명 확인 인증서도 작성하여 관리할 수 있습니다. 그리고 DCM이나 해당 API를 사용하여 오브젝트에 서명한 다음에 오브젝트의 서명을 확인할 수 있습니다.
- **디지털로 서명한 오퍼레이팅 시스템**
  V5R1부터 OS/400과 IBM LPP는 IBM에 의해 디지털로 서명이 이루어집니다. 따라서 IBM이 서명한 이후에는 IBM이 제공하는 프로그램이 변경되지 않은 것임을 확인할 수 있습니다. 디지털 서명 확인은 복원 시 또는 CHKOBJITG 명령을 실행할 때 수행됩니다. 또한 고객과 사업 파트너가 어플리케이션을 디지털로 서명하고 확인할 때에도 API를 사용할 수 있습니다.
- **새로운 사용자 프로파일 암호 규칙(QPWDLVL 2 및 3)**
  사용자 프로파일 암호 길이가 1에서 128자까지 늘어났습니다. 암호는 대소문자를 구분하며 공백이 허용됩니다(예: ″This is my New Password.″). 끝에 오는 공백은 제거되며 암호 전체를 공백으로 만들 수는 없습니다.
- **사용자 프로파일 암호 확장 기능**
  새 시스템값 QPWDLVL로 네 가지 옵션 중 하나를 설정하여 시스템의 암호 레벨을 제어할 수 있습니다.
  - PWDLVL 0 -- 이 설정 값은 암호 길이에 10바이트를 허용하고 Netserver 암호를 보유합니다. 이것이 디폴트 설정 값입니다.
  - PWDLVL 1 -- 이 설정 값은 암호 길이에 10바이트를 허용하고 Netserver 암호를 삭제합니다.
  - PWDLVL 2 -- 이 설정 값은 암호 길이에 128자를 허용하고, 기존 암호 형식과 새 암호 형식에 모두 맞는 암호를 보유합니다.
  - PWDLVL 3 -- 이 설정 값은 암호 길이에 128자를 허용하고, 기존 암호 형식을 삭제합니다.
- **더 안전하게 키를 저장하기 위한 IBM 4758-023 PCI 암호 코프로세서 지원**
  시스템에 IBM 4758-023 PCI 암호 코프로세서가 설치되어 있으면 그것을 사용하여 더 안전하게 디지털 인증을 저장할 수 있습니다. DCM을 사용하여 인증서를 작성하거나 갱신할 때, 키를 코프로세서에 직접 저장하거나 코프로세서 마스터 키로 개인

키를 암호화하여 특별한 키 저장 파일에 저장할 수 있습니다. 또한 키를 저장하기 위해 코프로세서를 사용할 경우 SSL 작동 가능 어플리케이션에 대한 SSL 성능을 향상시킬 수 있습니다. 이것은 코프로세서가 SSL 핸드쉐이크에 제공할 개인 키의 해독 타스크를 처리하기 때문입니다. 또한 여러 4758 카드에서 처리되는 SSL 핸드쉐이크의 로드 균형 조절 작업을 처리할 수도 있습니다.

- **VPN(가상 사설망) 인증 지원**
  V5R1 이전에는 사전 공유 키를 사용해야만 VPN IKE(인터넷 키 교환) 서버를 서로 인증할 수 있었습니다. 사전 공유 키를 사용하는 것은 이 키를 VPN의 반대쪽 종료점에 있는 관리자에게 수동으로 전달해야 하기 때문에 덜 안전합니다. 따라서 키 전달 프로세스 중에 키가 다른 사람에게 노출될 가능성이 있었습니다. V5R1에서는 사전 공유 키를 사용하는 대신에 디지털 인증을 통해 종료점을 인증함으로써 이런 위험을 피할 수 있습니다. 디지털 인증 관리자(DCM)를 사용하여 IKE 서버가 동적 VPN 연결 설정에 사용하는 인증서를 관리할 수 있습니다.
- **SSL 작동 가능 어플리케이션 개선사항**
  V5R1에는 SSL 확장 기능이 많이 있습니다. 이제 보안 통신 세션에 SSL을 사용하도록 iSeries FTP(파일 전송 프로토콜) 서버를 구성할 수 있습니다. 또한 FTP 서버를 구성하여 클라이언트 인증에 디지털 인증을 사용할 수 있습니다. 뿐만 아니라 V5R1에서는 OS/400이 128비트 AES 암호 지원을 제공합니다. AES는 DES 알고리즘을 대신하는 새롭고 빠른 암호화 알고리즘입니다.
- **SMTP(Simple Mail Transfer Protocol) 확장 기능**
  이제 SMTP가 제목, 송신자 및 IP 주소를 기반으로 블랙리스트 지원을 제공합니다.
- **인터넷 설치 마법사**
  다운로드할 수 있는 파일로서 최근에 출시된 인터넷 설치 마법사를 Operations Navigator 안에서 직접 사용할 수 있게 되었습니다. 마법사를 사용하여 iSeries 시스템에 맞게 인터넷 연결을 구성하고, 자동으로 생성되는 필터 규칙을 사용하여 보안할 수 있습니다.
- **프로그램 작성 자료 보존 확장 기능**
  V5R1 이상의 iSeries 시스템용으로 작성된 프로그램에는 필요에 따라 복원 시에 프로그램을 다시 작성할 수 있게 해주는 정보가 들어 있습니다. 프로그램을 다시 작성하는 데 필요한 정보는 프로그램의 Observability가 제거되어도 프로그램에 그대로 남아 있습니다. 프로그램이 복원될 때 프로그램 유효성 오류가 있는 것으로 판별되면 프로그램 유효성 오류를 수정하기 위해 프로그램이 다시 작성됩니다. 복원 시에 프로그램을 다시 작성하는 작업은 V5R1 iSeries에서의 새로운 기능이 아닙니다. 이전 릴리스에서는 복원 시 프로그램 유효성 오류가 발생하면 경우에 따라서(복원 중인 프로그램에 Observability가 있는 경우) 프로그램이 다시 작성되었습니다. V5R1 iSeries 이상의 프로그램에서 볼 수 있는 차이점은 Observability가 프로그램에서 제거되더라도 프로그램을 다시 작성하는 데 필요한 정보가 그대로 남는다는 점입니다. 그러므로 유효성 오류가 감지된 V5R1 이상의 프로그램의 경우 복원 중에 프로그램이 다시 작성되며, 유효성 오류를 발생시킨 변경 처리가 제거됩니다.

제 2 장 이 주제 인쇄

보기 또는 인쇄를 위해 이 문서의 PDF 버전을 보거나 다운로드할 수 있습니다. PDF 파일을 보려면 Adobe Acrobat Reader를 설치해야 합니다. Adobe 홈 페이지에서 다운로드 받을 수 있습니다. 

PDF 버전을 보거나 다운로드하려면 IBM SecureWay: iSeries 및 인터넷(416KB 또는 60 페이지)을 선택하십시오.

워크스테이션에 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 여십시오(위의 링크 클릭).
2. 브라우저 메뉴에서 **파일**을 클릭하십시오.
3. **다른 이름으로 저장...**을 클릭하십시오.
4. PDF를 저장할 디렉토리로 이동하십시오.
5. **저장**을 클릭하십시오.

제 3 장 iSeries 400 및 인터넷 보안

시스템을 인터넷에 연결하기 위해 옵션을 탐색 중인 iSeries 400 소유자들이 일반적으로 처음 갖는 질문 중 하나는 ″인터넷을 업무에 어떻게 사용할 것인가?″하는 것입니다. 두 번째 질문은 ″보안과 인터넷에 대해 알아야 할 것은 무엇인가?″하는 것입니다. 여기에서는 두 번째 질문에 대한 답을 중심으로 설명합니다.

″보안과 인터넷에 대해 알아야 할 것은 무엇인가?″라는 질문에 있어서 그 답은 인터넷을 어떻게 사용할 것인가에 달려 있습니다. 인터넷과 관련된 보안 문제는 매우 중요합니다. 사용자가 처리해야 할 사항은 인터넷 사용 계획을 어떻게 수립하는지에 따라 다릅니다. 인터넷으로 들어가는 첫 번째 작업은 내부 네트워크 사용자에게 웹과 인터넷 전자 우편에 대한 액세스를 제공하는 것입니다. 또한 한 사이트에서 다른 사이트로 중요한 정보를 전송할 수 있는 능력도 필요할 것입니다. 궁극적으로, e-commerce에 인터넷을 사용하거나 귀사, 협력업체, 공급업체 사이에 엑스트라넷을 작성할 계획일 수도 있습니다.

인터넷에 참여하기 위해서는 먼저 무엇을 할 것인지와 어떤 방법으로 그 일을 할 것인지에 관해 철저하게 생각해야 합니다. 인터넷 사용과 인터넷 보안을 동시에 결정하는 것은 복잡할 수 있습니다. 고유 인터넷 사용 계획을 개발할 때는 시나리오: JKL Toy사 e-비즈니스 계획 페이지를 검토하는 것이 도움이 될 것입니다. (주: 보안과 인터넷 관련 용어에 관해 익숙하지 않으면 본 자료를 읽는 중에 일반적인 보안 전문 용어를 검토하십시오.)

보안 문제와 사용 가능한 보안 툴, 기능, 오퍼링을 포함하여 e-business에 인터넷을 어떻게 사용할 것인지를 이해했으면 보안 정책과 목표를 개발할 수 있습니다. 많은 요소들이 보안 정책을 개발하기 위한 사용자의 선택에 영향을 줍니다. 보안 정책은 귀사를 인터넷으로 확장시킬 때 귀사의 시스템과 자원을 안전하게 보장하기 위한 중요한 기초가 됩니다.

iSeries 400 시스템 보안 특성

인터넷에서 시스템을 보호하기 위한 여러 가지의 보안 오퍼링 이외에도 iSeries 400에는 다음과 같은 매우 강력한 시스템 보안 특성이 있습니다.

- 다른 시스템에서 제공되는 추가 보안 소프트웨어 패키지와 비교하여 보안 처리를 우회하여 침입하는 것이 매우 어려운 통합 보안.
- 기술적으로 바이러스를 생성하여 전파하는 것을 어렵게 만든 오브젝트 기반 구조. iSeries에서는 파일을 프로그램으로 가장할 수 없으며, 프로그램을 또다른 프로그램으로 변경할 수도 없습니다. iSeries 무결성 피처로 인해 사용자들은 시스템이 제공하는 인터페이스를 사용하여 오브젝트에 액세스해야 합니다. 시스템에서의 그 주소

로 오브젝트에 직접 액세스할 수 없습니다. 오프셋을 포인터로 바꾸거나 포인터를 "생성"할 수 없습니다. 다른 시스템 구조의 경우 해커들이 가장 많이 사용하는 기술이 이 포인터 조작입니다.

- 사용자 고유의 요구사항에 맞게 시스템 보안을 설정할 수 있는 융통성. Technical Studio Security Advisor  를 이용하여 보안 요구에 맞는 보안 권장사항을 판별할 수 있습니다.

iSeries 확장 보안 오퍼링

iSeries는 인터넷과의 연결 시 시스템 보안을 확장하는 데 사용할 수 있는 여러 가지 특정 보안 오퍼링도 제공합니다. 인터넷을 사용하는 방법에 따라서 다음 중 하나 이상을 사용할 수 있습니다.

- VPN(가상 사설망)은 인터넷과 같은 공용 네트워크를 통해 기업의 사설 인트라넷을 확장한 것입니다. 기본적으로 공용 네트워크에 사설 "터널"을 작성하여 보안된 사설 연결망을 작성하기 위해 VPN을 사용할 수 있습니다. VPN은 Operations Navigator 인터페이스에서 제공하는 OS/400의 통합 피처입니다.
- 패킷 규칙은 Operations Navigator 인터페이스에서 제공하는 OS/400의 통합 피처입니다. 이 피처를 사용하여 IP 패킷 필터와 NAT(네트워크 주소 변환) 규칙을 구성함으로써 iSeries 시스템으로 들어가고 나오는 TCP/IP 통신 흐름을 제어할 수 있습니다.
- 보안 소켓층(SSL) 어플리케이션 통신 보안은 서버 어플리케이션과 클라이언트 사이에 보안 연결을 구축할 때 SSL을 사용하는 어플리케이션을 구성할 수 있게 합니다. SSL은 원래 웹 브라우저와 서버 어플리케이션 보안용으로 개발된 것이지만, 다른 어플리케이션들도 사용할 수 있습니다. 이제 iSeries용 IBM HTTP Server, Client Access Express, FTP(파일 전송 프로토콜), Telnet 등을 포함하여 많은 iSeries 서버 어플리케이션을 SSL에서 작동할 수 있습니다.

보안 문제, 사용할 수 있는 보안 툴, 기능, 오퍼링을 포함하여 인터넷을 어떻게 사용할 것인지를 이해했다면, 보안 정책 및 목표를 개발할 준비가 완료된 것입니다. 많은 요소들이 보안 정책을 개발하기 위한 사용자의 선택에 영향을 줍니다. 귀사를 인터넷으로 확장시킬 때 보안 정책이 귀사의 시스템을 안전하게 만들기 위한 중요한 초석을 제공합니다.

주: 인터넷을 귀사의 업무에 사용하는 방법에 대한 자세한 정보는 온라인 Information Center 주제 및 IBM 레드북을 검토하십시오.

- *인터넷 연결*
- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929). 

제 4 장 인터넷 보안 계획

인터넷 사용 계획을 수립할 때, 반드시 인터넷 보안 요구를 주의깊게 계획하십시오. 또한 인터넷 사용 계획에 대한 자세한 정보를 수집하고 내부 네트워크 구성을 문서로 정리하십시오. 수집된 정보를 기초로 보안 요구를 정확히 평가할 수 있습니다.

예를 들어, 다음과 같은 사항을 문서로 정리하여 설명해야 합니다.

- 현재 네트워크 구성
- DNS 및 전자 우편 서버 구성 정보
- 인터넷 서비스 제공자(ISP)와의 연결
- 인터넷에서 사용할 서비스
- 인터넷 사용자에게 제공할 서비스

이와 같은 유형의 정보를 문서로 정리함으로써 보안이 노출되어 있는 곳은 물론 노출을 최소화하기 위해 어떤 보안 수단을 사용해야 할 것인지를 알 수 있습니다.

예를 들어, 내부 사용자들이 특수 연구 지역의 호스트에 연결할 때 Telnet을 사용하는 것을 허용하려고 합니다. 내부 사용자들은 회사의 새로운 제품을 개발하는 데 도움을 받기 위해 이 서비스가 필요합니다. 그러나 보안되지 않은 상태로 인터넷을 통해 흐르는 기밀 자료에 대한 몇 가지 문제를 느끼고 있습니다. 만일 경쟁사가 이 자료를 가로채서 이용한다면 자사에 금전적으로 큰 손해를 입힐 수 있습니다. 사용 요구(Telnet) 및 관련 위험 요소(기밀 정보의 노출)를 확인함으로써 자료의 기밀성을 유지하기 위해 사용 시(SSL 사용 가능성) 구현해야 할 추가 보안 수단을 판별할 수 있습니다.

인터넷 사용과 보안 계획을 개발할 때 다음 주제를 검토하면 도움이 될 것입니다.

- **보안에 대한 계층적 방어 접근방식**은 포괄적인 보안 계획을 작성하는 것과 관련된 문제에 관해 자세한 정보를 제공합니다.
- **보안 정책과 목표** 에서는 포괄적인 보안 계획을 작성하는 것과 관련된 문제를 쉽게 이해하는 데 도움이 되는 정보를 제공합니다.
- **시나리오: JKL Toy사 e-비즈니스 계획**은 귀사의 계획을 작성할 때 사용할 수 있는 전형적인 기업 인터넷 사용 및 보안 계획에 대한 실제 모델을 제공합니다.

더 이상 공급되지 않는 제품이라 할지라도 계획을 문서화하는 데 IBM Firewall for AS/400 계획 작업용지를 변경해서 사용하는 것이 도움이 될 것입니다. 이 작업용지는 인터넷 사용 계획 및 내부 네트워크 구성에 관한 상세하고 중요한 정보를 수집하는 데 도움을 줄 뿐만 아니라 보안 요구를 평가하는 데에도 유용합니다. V4R5 iSeries Information Center의 방화벽: 시작하기 주제에서 이 작업용지에 액세스할 수 있습니다. 방화벽 제품의 사용 여부와 관계없이 인터넷 보안 전략을 계획하기 위해서는 같은 자료를 많이 수집해야 합니다.

보안에 대한 계층적 방어 접근방식

보안 정책은 사용자가 보호하려는 것과 시스템 사용자에게서 기대하는 것을 정의한 것입니다. 이 보안 정책이 새로운 어플리케이션을 설계하거나 현재 네트워크를 확장할 때 보안 계획을 위한 기초를 제공합니다. 또한 기밀 정보를 보호하는 것과 추측하기 어려운 암호를 작성하는 등과 같은 사용자 책임사항을 기술합니다.

주: 내부 네트워크에 대한 위험을 최소화하도록 귀사의 보안 정책을 작성하고 실시해야 합니다. iSeries 400 고유의 보안 피처를 올바로 구성할 경우 많은 위험을 최소화할 수 있는 능력을 제공받을 수 있습니다. 그러나 iSeries 시스템을 인터넷에 연결할 때는 내부 네트워크의 안전을 보장하기 위한 추가 보안 수단을 제공해야 합니다.

인터넷 액세스를 사용하여 업무 활동을 수행하는 것에는 많은 위험이 따릅니다. 보안 정책을 작성할 때는 기능 및 자료의 액세스를 제어하는 것에 대하여 서비스를 제공하는 것과의 균형이 필요합니다. 네트워크로 연결된 컴퓨터에서는 통신 채널 자체가 공격을 받기 쉽기 때문에 보안에 더 큰 어려움이 있습니다.

일부 인터넷 서비스의 경우 다른 서비스보다 특정 공격 유형에 대해 더욱 취약한 면이 있습니다. 그러므로 사용하거나 제공할 각 서비스에 따르는 위험 요소를 이해하는 것이 중요합니다. 뿐만 아니라, 잠재적인 보안 위험요소를 이해함으로써 확실한 보안 목표를 수립할 수 있습니다.

인터넷은 인터넷 통신 보안에 위협을 가할 수 있는 다양한 사람들이 존재하는 장소입니다. 다음은 발생할 가능성이 있는 대표적인 몇 가지의 보안 위험요소를 나열한 것입니다.

- **수동적 공격**: 수동적 공격에서는 침입자가 비밀을 알기 위해 단지 네트워크 통신을 모니터합니다. 그와 같은 공격은 네트워크 기반 공격(통신 링크 추적) 또는 시스템 기반 공격(시스템 구성요소를 트로이 목마 프로그램(아무도 모르게 자료를 캡처하는)으로 대체) 중 하나일 수 있습니다. 수동적 공격이 감지하기가 가장 어렵습니다. 그러므로 사용자가 인터넷을 통해 송신하는 모든 것은 누군가에 의해 도청당하고 있는 것으로 생각해야 합니다.
- **능동적 공격:** 능동적 공격에서는 침입자가 사용자의 방어막을 뚫고 네트워크 시스템에 침입하려고 시도합니다. 능동적 공격에는 다음과 같은 여러 가지 유형이 있습니다.
  - **시스템 액세스 시도**의 경우, 공격자는 클라이언트나 서버 시스템에 대한 액세스와 제어를 얻기 위해 보안 상의 허점을 이용하려고 시도합니다.
  - **가장** 공격에서는 공격자가, 신뢰할 수 있는 시스템으로 가장하여 방어를 돌파하거나 사용자를 설득하여 자신에게 비밀 정보를 송신하도록 합니다.
  - **서비스 거부 공격**에서는 공격자가 통신 흐름을 바꾸거나 잡동사니 정보로 공세를 가함으로써 사용자 작업을 간섭하거나 시스템을 중단(shut down)시키려고 합니다.

– **암호 공격**에서는 공격자가 사용자 암호를 추측하거나 훔치거나 암호화된 자료를 해독하기 위해 특별한 툴을 사용합니다.

다중 방어층

여러 레벨에서 잠재적인 인터넷 보안 위험요소가 발생할 수 있으므로 이러한 위험요소에 대비하여 다중 방어 계층의 보안 수단을 설정해야 합니다. 일반적으로 인터넷에 연결할 때 침입 시도나 서비스 거부 공격이 **발생하더라도** 이상하게 생각하지 마십시오. 그 대신, 보안 문제가 **발생할** 것에 대비하십시오. 결과적으로, 최상의 방어는 철저한 적극적인 방어입니다. 인터넷 보안 전략을 계획할 때 계층적 접근을 사용하면 하나의 방어층을 침투한 공격자를 그 다음 계층에서 중단시킬 수 있습니다.

보안 전략에는 다음과 같은 전통적 네트워크 컴퓨팅 모델 계층에 있어서 보호를 제공하는 수단을 포함시켜야 합니다. 일반적으로, 가장 기본적인 레벨(시스템 레벨 보안)부터 가장 복잡한 레벨(트랜잭션 레벨 보안)까지 보안을 계획해야 합니다.

시스템 레벨 보안

시스템 보안 수단은 인터넷 기반 보안 문제에 있어서 마지막 방어선을 의미합니다. 따라서 전체 인터넷 보안 전략의 첫 번째 단계는 iSeries 기본 시스템 보안 설정을 올바로 구성하는 것입니다.

네트워크 레벨 보안

네트워크 보안 수단은 iSeries 및 기타 네트워크 시스템에 대한 액세스를 제어합니다. 네트워크를 인터넷에 연결할 때, 권한이 없는 액세스 및 침입으로부터 내부 네트워크 자원을 보호하기 위해서는 적절한 네트워크 레벨 보안 수단이 필요합니다. 방화벽은 네트워크 보안을 위한 가장 일반적인 수단입니다. 인터넷 서비스 제공자(ISP)가 네트워크 보안 계획에 있어서 중요한 요소를 제공할 수 있으며 반드시 제공해야 합니다. 귀사의 네트워크 보안 체계는 ISP 라우터 연결 및 공용 DNS(정의역명 서비스) 사전 주의사항에 대한 필터링 규칙 등과 같이 ISP가 제공할 보안 수단을 개괄적으로 기술하는 것이어야 합니다.

어플리케이션 레벨 보안

어플리케이션 레벨 보안 수단은 사용자들이 특정 어플리케이션과 대화하는 방법을 제어합니다. 일반적으로, 사용하는 각 어플리케이션에 대해 보안 설정을 구성해야 합니다. 그러나 인터넷에서 제공받아 사용하거나 인터넷에 제공하는 어플리케이션과 서비스에 대해서는 보안 설정에 특히 주의해야 합니다. 이와 같은 어플리케이션과 서비스는 사용자의 네트워크 시스템에 액세스하기 위해 방법을 찾고 있는 권한이 없는 사용자의 오용에 매우 취약합니다. 사용하기로 결정한 보안 수단은 서버와 클라이언트 양쪽에서 보안 노출 문제를 모두 다루어야 합니다.

전송 레벨 보안

전송 레벨 보안 수단은 네트워크 내부나 네트워크 간의 자료 통신을 보호합니다. 인터넷과 같이 신뢰할 수 없는 네트워크를 통해 통신이 이루어질 때는 통신이 소스에서 목적지를 향해 흐르는 방법을 제어할 수 없습니다. 통신과 그 통신에 의해 운반되는 자료는 사용자가 제어할 수 없는 많은 수의 서로 다른 서버를 통해 흐릅니다. 보안 소켓층(SSL)을 사용하도록 어플리케이션을 구성하는 것과 같은 보안 수단을 설정하지 않으면, 라우트되는 자료를 누군가가 보고 사용할 수 있습니다. 전송 레벨 보안 수단은 다른 한쪽의 보안 레벨 경계를 지나 자료가 흐를 때 보호를 제공합니다.

전체적인 인터넷 보안 정책을 수립할 때는 각 계층별로 보안 전략을 수립해야 합니다. 또한 각각의 전략 세트가 나머지 전략 세트와의 대화를 통해 귀사의 업무 전반에 걸쳐 포괄적인 보안 안전망을 제공하도록 하기 위한 방법에 관해서도 설명해야 합니다.

보안 정책과 목표

보안 정책

인터넷에서 사용하는 서비스나 인터넷으로 제공하는 서비스 모두 iSeries 시스템과 그 시스템이 연결되어 있는 네트워크에 위험을 초래합니다. 보안 정책은 귀사에 속하는 컴퓨터와 통신 자원을 위한 활동에 적용되는 규칙 세트입니다. 이 규칙들이 물리적 보안, 개인 보안, 관리 보안 및 네트워크 보안과 같은 영역을 처리합니다.

보안 정책은 사용자가 보호하려는 것과 시스템 사용자에게서 기대하는 것을 정의한 것입니다. 이 보안 정책이 새로운 어플리케이션을 설계하거나 현재 네트워크를 확장할 때 보안 계획을 위한 기초를 제공합니다. 또한 기밀 정보를 보호하는 것과 추측하기 어려운 암호를 작성하는 등과 같은 사용자 책임사항을 기술합니다. 보안 정책에는 보안 수단의 효율성을 모니터하기 위한 방법에 대해서도 설명이 필요합니다. 그와 같은 모니터링을 통해 사용자의 보호막을 피해가려고 시도하는 사람이 있는지 판별할 수 있습니다.

보안 정책을 수립하기 위해서는 반드시 보안 목표를 명확하게 정의해야 합니다. 그리고 보안 정책을 작성했으면, 보안 정책에 포함된 규칙이 효력을 나타내도록 필요한 단계를 취해야 합니다. 이와 같은 단계에는 사원 교육을 포함하여 규칙을 시행하기 위해 필요한 소프트웨어 및 하드웨어 추가 처리가 있습니다. 또한 컴퓨팅 환경을 변경할 때는 보안 정책도 따라서 갱신해야 합니다. 이것은 변경으로 인해 발생할 수 있는 모든 새로운 위험에 대비하기위한 것입니다. iSeries Information Center의 ″기본 시스템 보안 및 계획″ 주제에서 JKL Toy사의 보안 정책에 대한 예를 찾을 수 있습니다.

보안 목표

보안 정책을 작성하고 수행할 때는 명확한 목표가 필요합니다. 다음 중 하나 이상의 범주에 보안 목표를 맞출 수 있을 것입니다.

자원 보호

자원 보호 체계는 권한이 있는 사용자만 시스템 오브젝트에 액세스하는 것을 보장합니다. 모든 유형의 시스템 자원을 보호할 수 있는 능력이 iSeries의 강점입니다. 시스템에 액세스할 수 있는 사용자들을 여러 범주로 분류하여 세심하게 정의해야 합니다. 또한 보안 정책을 작성하는 작업의 일부로 사용자 그룹별로 제공할 액세스 권한을 정의해야 합니다.

인증 세션의 다른 쪽 끝에 있는 자원(사람 또는 기계)이 실제로 권한이 있는 것임을 보장하거나 검증하는 것. 확실한 인증은 송신자나 수신자가 시스템에 액세스하기 위해 거짓 신분을 사용함으로써 발생할 수 있는 위장 보안 위험요소에 대해 시스템을 보호합니다. 일반적으로, 인증을 위해 시스템에서는 암호와 사용자명을 사용하며 디지털 인증을 통해 기타 보안 상의 이점은 물론 더욱 안전한 인증 방법을 제공할 수 있습니다. 시스템을 인터넷과 같은 공용 네트워크에 연결할 때, 사용자 인증은 새로운 중요성을 나타냅니다. 인터넷과 인트라넷의 중요한 차이점은 사인 온(Sign On)하는 사용자의 신분을 신뢰할 수 있는 능력입니다. 따라서, 전통적인 사용자명과 암호 로그온 프로시듀어가 제공하는 것보다 더 강력한 인증 방법을 사용할 것을 신중히 고려해야 합니다. 인증된 사용자들은 권한 부여 레벨에 따라서 서로 다른 허가 유형을 가질 수 있습니다.

권한 부여

세션의 다른 쪽 끝에 있는 사람이나 컴퓨터가 요구를 수행할 수 있는 허가를 갖고 있음을 보장하는 것. 권한 부여는 시스템 자원에 액세스하거나 시스템에서 특정 활동을 수행할 수 있는 사람이나 자원을 판별하는 프로세스입니다. 대개, 권한 부여는 인증의 맥락에서 수행됩니다.

무결성

수신 정보가 송신 정보와 동일한 것임을 보장하는 것. 무결성을 이해하기 위해서는 자료 무결성과 시스템 무결성 개념을 이해해야 합니다.

- **자료 무결성**: 자료를 권한이 없는 변경이나 간섭으로부터 보호합니다. 자료 무결성은 권한이 없는 누군가가 정보를 가로채서 변경하는 불법 조작의 보안 위험에 대해 보호를 제공합니다. 네트워크 안에 저장되어 있는 자료를 보호하는 것에 추가하여, 신뢰할 수 없는 소스로부터 시스템으로 자료가 들어올 때 자료 무결성을 보장하는 추가

보안이 필요할 수 있습니다. 시스템에 들어오는 자료가 공용 네트워크에서 오는 것이면, 다음을 수행하기 위한 보안 방법이 필요할 수 있습니다.

- 일반적으로 자료를 암호화하여 자료가 『유출』되고 해석되지 않도록 보호합니다.
- 전송된 자료가 수정되지 않았음(자료 무결성)을 보장합니다.
- 전송이 발생했음(비거부)을 증명합니다. 미래에는 등기 우편이나 내용 증명 우편과 같은 전자 우편이 필요할지 모릅니다.

- **시스템 무결성**: 시스템이 예상 성능으로 일관성있게, 예상 결과를 제공합니다. iSeries의 경우, 시스템 무결성이 iSeries 구조에 있어서 기본적인 부분을 구성하기 때문에 일반적으로 가장 간과하기 쉬운 보안 구성요소입니다. 예를 들어, iSeries 구조에서는 보안 레벨 40이나 50의 경우 사용자가 오퍼레이팅 시스템 프로그램을 모방하거나 변경하기가 매우 어렵습니다.

비거부(Non-repudiation)

비거부는 트랜잭션이 발생했음, 메세지를 전송했음 또는 메세지를 수신했음을 증명하는 것입니다. 트랜잭션, 메세지, 문서에 대한 ″서명″을 위해 디지털 인증서와 공용 키 암호를 사용할 때 비거부가 지원됩니다. 송신자와 수신자 모두가 교환이 발생한 것에 동의합니다. 자료에 대한 디지털 서명이 필요한 증거를 제공합니다.

기밀성 민감한 정보를 사적인 상태로 유지하여 도청자가 보지 못하도록 보장하는 것입니다. 기밀성은 자료 전체 보안에 매우 중요한 요소입니다. 디지털 인증과 보안 소켓층(SSL)을 사용하여 자료를 암호화하면 신뢰할 수 없는 네트워크 간의 자료 전송에 있어서 기밀성이 보장됩니다. 보안 정책은 네트워크 안에서 뿐만 아니라 정보가 네트워크를 벗어나더라도 정보의 기밀성을 유지하기 위한 방법을 지정해야 합니다.

보안 활동 감사

성공한 액세스와 실패한(거부당한) 액세스 모두의 기록부를 제공하기 위한 보안 관련 이벤트 모니터링. 성공한 액세스 레코드는 시스템에서 누가 무엇을 수행 중인지를 알려줍니다. 실패한(거부당한) 액세스 레코드는 누군가가 보안을 파괴하려고 시도 중이거나 시스템에 액세스하는 데 어려움을 겪고 있음을 알려줍니다.

보안 목표를 이해함으로써 모든 네트워킹 및 인터넷 보안 요구를 처리하는 보안 정책을 작성하는 데 도움을 받을 수 있습니다. 목표를 정의하고 보안 정책을 작성할 때 JKL Toy사 e-비즈니스 시나리오를 검토하면 도움이 될 것입니다. 이 회사의 인터넷 사용 및 보안 계획 시나리오는 실제로 여러 기업에서 발생하는 예를 나타낸 것입니다.

시나리오: JKL Toy사 e-비즈니스 계획

이 시나리오에는 일반적인 기업, JKL Toy사가 나옵니다. 이 회사에서는 인터넷을 사용하여 사업 목표를 확장하기로 결정했습니다. 물론 이 회사는 가공의 회사지만, e-비즈니스를 위한 인터넷 사용 계획과 이로 인해 발생하는 보안 요구는 다른 많은 실제 회사의 상황을 나타내는 것으로 볼 수 있습니다.

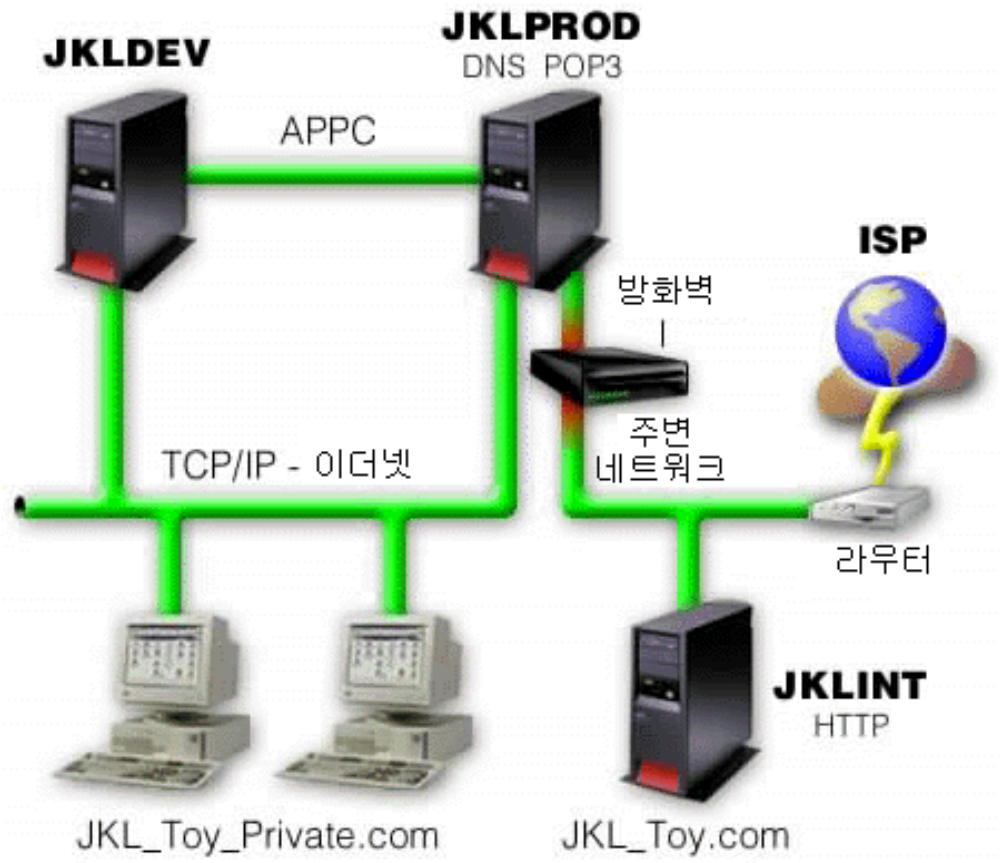
JKL Toy사는 규모는 적지만 빠르게 성장하는 장난감 제조업체로서 줄넘기부터 연과 귀여운 표범 인형까지 모든 완구를 생산합니다. 이 회사의 회장은 사업 확장으로 인한 부담을 자사의 신규 iSeries 시스템을 이용하여 해결할 수 있는 방안을 모색하는 중입니다. 재정 관리자, Sharon Jones가 iSeries 시스템 관리와 시스템 보안을 담당하고 있습니다.

JKL Toy사는 일 년이 지나도록 내부 어플리케이션을 위한 보안 정책을 성공적으로 사용해 오고 있습니다. 회사에서는 이제 내부 정보를 보다 효율적으로 공유하기 위해 인트라넷을 구축하려고 합니다. 또한 사업 목표를 추진하기 위해 인터넷을 사용하려고 계획 중입니다. 이러한 목표에는 온라인 카탈로그를 포함하여 기업 인터넷 마케팅 업무를 추진할 계획도 포함됩니다. 또한 인터넷을 사용하여 원격지에서 본사로 중요한 정보를 전송하려고 합니다. 그리고 디자인실의 직원들이 연구 및 개발을 목적으로 인터넷에 액세스할 수 있게 하려고 합니다. 궁극적으로는 고객들이 웹 사이트를 이용하여 직접 온라인 구매를 할 수 있게 하려고 합니다. Sharon은 이러한 모든 활동에 있어서 발생할 수 있는 잠재적인 보안 위험 요소와 이러한 위험을 최소화하기 위해 회사에서 사용해야 할 보안 수단에 관한 보고서를 작성 중입니다. Sharon은 회사 보안 정책을 갱신하고 회사에서 사용하기로 결정한 보안 수단을 시행하는 책임을 담당할 것입니다.

인터넷 관련 업무의 목표는 다음과 같습니다.

- 전반적인 마케팅 캠페인의 일부로서 일반적인 기업 이미지와 업무를 홍보합니다.
- 고객과 영업팀을 위한 온라인 제품 카탈로그를 제공합니다.
- 고객 서비스를 개선합니다.
- 직원 전자 우편과 WWW 액세스를 제공합니다.

JKL Toy사에서는 iSeries 시스템에 기본적인 강력한 시스템 보안 체계를 구축한 다음, 네트워크 레벨 보호를 제공하는 방화벽 제품을 구입해서 사용하기로 결정했습니다. 방화벽은 잠재적인 인터넷 관련 위험 요소로부터 내부 네트워크를 보호할 것입니다. 아래는 회사 인터넷/네트워크 구성의 그림입니다.



다이어그램에서 보는 것처럼 JKL Toy사에는 두 개의 1차 iSeries 시스템이 있습니다. 두 시스템 중 하나는 시스템(JKLDEV) 개발용으로 그리고 다른 하나(JKLPROD)는 생산 어플리케이션용으로 사용합니다. 두 시스템 모두 업무에 중요한 자료와 어플리케이션을 처리합니다. 따라서, 이 시스템에서는 인터넷 어플리케이션을 실행하지 않으려고 합니다. 그 대신, 이 어플리케이션을 실행할 새로운 iSeries 시스템(JKLINT)을 추가하기로 결정했습니다.

회사는 신규 시스템을 주변 네트워크에 배치했으며 내부 네트워크와 인터넷을 더욱 안전하게 분리하기 위해 신규 시스템과 회사의 기본 내부 네트워크 사이에 방화벽을 사용하려고 합니다. 이러한 분리는 내부 시스템이 취약한 면을 드러내는 인터넷 위험 요소들을 감소시킵니다. 또한 회사에서는 신규 iSeries를 인터넷 서버 전용으로 지정하여 네트워크 보안 관리의 복잡성을 줄였습니다.

신규 iSeries 시스템에서는 중요한 업무용 어플리케이션을 실행시키지 않을 것입니다. e-비즈니스 계획 중 이 단계에서는 신규 시스템이 정적 공용 웹 사이트만 제공할 것입니다. 그러나 회사에서는 서비스 중단이나 기타 발생할 가능성이 있는 공격을 방지하기 위해 시스템 자체를 포함하여 그 시스템에서 실행하는 공용 웹 사이트를 보호할 수 있는

보안 수단을 구현하려고 합니다. 궁극적으로, 회사에서는 기본적인 강력한 보안 수단 뿐 아니라 패킷 필터링 규칙과 네트워크 주소 변환(NAT) 규칙으로 시스템을 보호할 것입니다.

회사에서 보다 확장된 공용 어플리케이션(예: 전자상거래용 웹 사이트 또는 외부 네트워크 액세스)을 개발하면 할수록 보다 확장된 보안 수단을 구축해야 할 것입니다.

제 5 장 기본 인터넷 준비를 위한 보안 레벨

시스템 보안 수단은 인터넷 기반 보안 문제에 있어서 마지막 방어선을 의미합니다. 따라서 전체적인 인터넷 보안 전략의 첫 단계는 OS/400 기본 보안 설정을 올바르게 구성하는 것이어야 합니다. 다음과 같이 하여 시스템 보안에 있어서 최소한의 요구사항을 반드시 충족시켜야 합니다.

- 보안 레벨(QSECURITY 시스템 값)을 50으로 설정하십시오. 보안 레벨 50은 인터넷과 같은 위험이 높은 환경에서 시스템을 보호하는 데 적합한 최상위 레벨의 무결성 보호를 제공합니다.

  주: 트랜잭션 중심의 어플리케이션이나 통합 파일 시스템을 집중적으로 사용하는 어플리케이션이 있을 때 보안 레벨 50에서 작동시키면 시스템이나 어플리케이션의 성능이 저하될 수 있습니다.

  각 iSeries 보안 레벨에 대한 자세한 내용은 iSeries 보안을 위한 추가 정보 및 툴

  
  을 참조하십시오.

  주: 현재 50 이하의 보안 레벨에서 실행 중이면 운영 프로시듀어나 어플리케이션을 갱신해야 할 수 있습니다. 더 높은 보안 레벨로 변경하기 전에 iSeries 보안 참조서 
  에 있는 내용을 검토하십시오.
- 보안 관련 시스템 값을 적어도 권장 설정 값에 해당하는 제한적인 값으로 설정하십시오. Operations Navigation 보안 마법사 또는 Technical Studio 보안 어드바이저를 사용하여 해당 설정 값을 권장 설정 값과 비교할 수 있습니다.
- IBM 제공 사용자 프로파일을 포함하여 사용자 프로파일이 디폴트 암호를 사용하지 않도록 하십시오. ANZDFTPWD(디폴트 암호 분석) 명령을 사용하여 디폴트 암호가 있는지 검사하십시오.
- 중요한 시스템 자원을 보호하기 위해 오브젝트 권한을 사용하십시오. 시스템에서 제한적 접근방식을 적용하십시오. 즉, 기본적으로 라이브러리나 디렉토리와 같은 시스템 자원에 대해 모든 사람을 제한하십시오(PUBLIC *EXCLUDE). 소수의 사용자들만 이러한 제한된 자원에 액세스할 수 있도록 허용하십시오. 메뉴를 통한 액세스 제한만으로는 인터넷 환경에서 충분하지 않습니다.
- **반드시** 시스템에 오브젝트 권한을 설정하십시오. 오브젝트 권한 작업에 대한 자세한 내용은 iSeries 보안을 위한 추가 정보 및 툴 
의 iSeries Navigator 장을 참조하십시오.

이러한 최소 시스템 보안 요구사항을 구성할 때 **보안 어드바이저**(Technical Studio 웹 사이트에서 받을 수 있음) 또는 **보안 마법사**(iSeries Navigator 인터페이스에서 받을 수

있음)를 사용할 수 있습니다. Technical Studio 보안 어드바이저  는 일련의 질문에 대한 대답을 기초로 보안 권장사항을 제공합니다. 그런 다음, 이러한 권장사항을 사용하여 사용자가 필요한 시스템 보안 설정을 구성할 수 있습니다. 보안 마법사는 또한 일련의 질문에 대한 사용자 응답을 바탕으로 권장사항을 제공합니다. 그러나 보안 어드바이저와는 달리, 마법사가 권장사항을 사용하여 시스템 보안 설정을 구성하도록 할 수 있습니다.

iSeries 고유의 보안 피처를 올바로 구성하고 관리만 한다면 많은 위험 요소들을 최소화하는 능력을 제공받을 수 있습니다. 그러나 iSeries을 인터넷에 연결할 때는 내부 네트워크의 안전을 보장하기 위한 추가 보안 수단을 제공해야 합니다. iSeries에 일반적인 시스템 보안을 적절히 구현시켰으면 인터넷 사용을 위한 포괄적인 보안 계획의 일부로서 추가 보안 수단을 구성할 준비가 된 것입니다.

제 6 장 네트워크 보안 옵션

신뢰할 수 없는 네트워크에 연결할 때는 반드시 보안 정책이 네트워크 레벨에서 구현할 보안 수단을 포함하여 포괄적인 보안 체계를 설명하는 것이어야 합니다. 방화벽 설치는 포괄적인 네트워크 보안 수단 세트를 전개하는 가장 좋은 방법 중 하나입니다.

인터넷 서비스 제공자(ISP) 또한 귀사의 네트워크 보안 계획에 중요한 요소를 제공할 수 있으며 제공해야 합니다. 네트워크 보안 체계에는 ISP 라우터 연결을 위한 필터링 규칙이나 공용 DNS(정의역명) 예방 조치와 같이 ISP가 제공하는 보안 수단이 요약되어 있어야 합니다.

방화벽이 전체 보안 계획에 있어서 중추 역할을 하는 확실한 방어 장치의 하나라고 하더라도 **유일한** 방어 장치여서는 안됩니다. 여러 레벨에서 인터넷 보안 위험이 발생할 수 있으므로 이러한 위험에 대비한 다중 방위층의 보안 수단을 설정해야 합니다.

방화벽이 특정한 종류의 공격으로부터 상당한 보호를 제공하기는 하지만 전체 보안 솔루션의 일부에 지나지 않습니다. 예를 들어, 방화벽이 반드시 SMTP 메일, FTP 및 TELNET과 같은 어플리케이션을 통해 인터넷 상에서 송신되는 자료를 보호하는 것은 아닙니다. 이 자료를 암호화하도록 결정하지 않으면 자료가 목적지로 이동할 때 누구든지 인터넷에서 자료에 액세스할 수 있습니다.

iSeries 시스템이나 내부 네트워크를 인터넷에 연결할 때마다 방화벽 제품을 기본 방어 장치로 사용하는 문제를 적극 고려해야 합니다. IBM Firewall for AS/400 제품을 구입할 수 없거나 제품에 대한 지원이 더 이상 제공되지 않더라도 사용할 수 있는 다른 제품들이 많이 있습니다.

기존 IBM AS/400용 Firewall에서 기타 제품이나 iSeries 고유의 네트워크 보안 피처로 전환하는 것에 대한 내용은 All You Need to Know When Migrating from IBM Firewall for AS/400 (SG24-6152)을 참조하십시오.

상용 방화벽 제품들은 전방위의 네트워크 보안 기술을 반영하고 있으므로 JKL Toy사에서는 네트워크를 보호하기 위한 자사의 e-비즈니스 보안 시나리오에 그와 같은 방화벽 제품 중 하나를 사용하기로 결정했습니다. 그러나 자사의 방화벽이 신규 iSeries 인터넷 서버에 대해서는 전혀 보호를 제공하지 않습니다. 따라서, iSeries 패킷 규칙 피처를 구현하여 인터넷 서버의 통신을 제어하는 필터와 NAT 규칙을 작성하기로 결정했습니다.

iSeries 패킷 규칙 정보

패킷 필터 규칙은 사용자가 정의하는 범주에 따라서 IP 패킷을 거부하거나 수락하는 방식으로 컴퓨터 시스템을 보호합니다. NAT 규칙을 사용하여 하나의 IP 주소로 다른 공용 IP 주소를 대체하여 외부 사용자로부터 내부 시스템 정보를 숨길 수 있습니다. IP 패킷 필터와 NAT 규칙이 핵심적인 네트워크 보안 기술이라 할지라도 완벽하게 작동하는 방화벽 제품이 수행하는 것과 같은 수준의 보안을 제공하지는 못합니다. 완벽한 방화벽 제품과 iSeries 패킷 규칙 피처 중에서 하나를 결정해야 할 때는 보안 요구와 목표를 신중하게 분석해야 합니다.

iSeries 네트워크 보안 옵션 선택 주제를 검토하여 귀사의 보안 요구에 적합한 접근방식을 결정하십시오.

방화벽

방화벽은 안전한 내부 네트워크와 인터넷 등과 같이 신뢰할 수 없는 네트워크 사이의 차단막입니다. 다른 네트워크로부터 하나의 내부 네트워크를 보안하기 위해서 방화벽이 사용되기도 하지만 대부분의 회사에서는 내부 네트워크를 인터넷에 안전하게 연결하기 위해 방화벽을 사용합니다.

방화벽은 안전한 내부 네트워크와 신뢰할 수 없는 네트워크 사이에서 제어를 받는 하나의 연결점(초크점이라고 함)을 제공합니다. 방화벽의 기능은 다음과 같습니다.

- 내부 네트워크의 사용자들이 외부 네트워크의 권한이 있는 자원을 사용할 수 있게 합니다.
- 외부 네트워크의 권한이 없는 사용자가 내부 네트워크의 자원을 사용할 수 없게 합니다.

방화벽을 인터넷(또는 기타 네트워크)의 게이트웨이로 사용하면 내부 네트워크의 위험이 상당히 줄어듭니다. 방화벽 기능이 보안 정책 지시문의 대부분을 실행하기 때문에 방화벽을 사용하여 네트워크 보안을 쉽게 관리할 수 있습니다.

방화벽의 작동 방식

방화벽의 작동 방식을 이해하기 위해 네트워크를 사용자가 출입을 제어하는 건물로 가정하십시오. 건물에는 유일한 출입문으로 로비가 있습니다. 이 로비에는 방문객을 맞이하는 안내원, 방문객을 감시하는 보안 경비원, 방문객의 행동을 녹화하는 비디오 카메라, 건물로 들어오는 방문객을 인증하는 뱃지 판독기가 있습니다.

이와 같은 수단들이 잘 작동하면서 건물에 대한 출입을 제어할 수 있습니다. 그러나 권한이 없는 사람이 건물로 들어오는 데 성공할 경우 이 침입자로부터 건물을 보호할 방법이 없습니다. 그러나 침입자의 움직임을 모니터하면 침입자의 의심스러운 행동을 감지할 수 있습니다.

방화벽 구성요소

방화벽은 하드웨어와 소프트웨어의 콜렉션으로서 함께 사용되어 네트워크의 일부에 대한 권한이 없는 액세스를 방지합니다. 방화벽은 다음과 같은 구성요소로 이루어집니다.

- 하드웨어. 보통 방화벽 하드웨어는 별도의 컴퓨터나 방화벽 소프트웨어 기능을 실행하는 전용 장치로 구성됩니다.
- 소프트웨어. 방화벽 소프트웨어는 다양한 어플리케이션을 제공합니다. 네트워크 보안 측면에서 방화벽은 여러 가지 방법으로 이러한 보안 제어를 제공합니다.
  - 인터넷 프로토콜(IP) 패킷 필터링
  - NAT(네트워크 주소 변환) 서비스
  - SOCKS 서버
  - HTTP, Telnet, FTP 등과 같은 다양한 서비스에 대한 프록시 서버
  - 메일 릴레이 서비스
  - 분할 DNS(정의역명 서비스)
  - 기록
  - 실시간 모니터링

  주: 일부 방화벽들은 현재 사용하는 방화벽과 호환되는 기타 방화벽 사이에 암호화된 세션을 설정할 수 있도록 VPN(가상 사설망) 서비스를 제공합니다.

방화벽 기술 사용

방화벽 프록시 서버, SOCKS 서버 또는 NAT 규칙을 사용하여 내부 사용자들에게 인터넷 상의 서비스에 대한 안전한 액세스를 제공할 수 있습니다. 프록시 및 SOCKS 서버는 비보안 네트워크로부터 내부 네트워크 정보를 숨기기 위해 방화벽에서 TCP/IP 연결을 끊습니다. 또한 서버에서는 추가로 기록 기능도 제공합니다.

NAT를 사용하여 인터넷 사용자들이 방화벽 뒤에 있는 공용 서버에 쉽게 액세스하도록 할 수 있습니다. 방화벽은 NAT가 내부 IP 주소를 숨기므로 여전히 사용자 네트워크를 보호합니다.

또한 방화벽은 방화벽에 사용할 DNS 서버를 제공함으로써 내부 정보를 보호할 수 있습니다. 실제로 사용자에게는 DNS 서버 두 개가 있으며, 하나는 내부 네트워크에 대한 자료에 사용하는 서버이고, 다른 하나는 외부 네트워크와 방화벽 자체에 대한 자료에 사용하는 서버입니다. 이를 통해 내부 시스템 관련 정보에 대한 외부 액세스를 제어할 수 있습니다.

방화벽 전략을 정의할 때 보통은 조직에 위험하다고 간주되는 모든 것을 금지하고 그밖의 모든 것을 허용하면 충분한 것으로 생각하기 쉽습니다. 그러나 컴퓨터 범죄자들이 새로운 공격 방법을 지속적으로 만들어내기 때문에 이와 같은 공격들을 방지하는 방법이 필요합니다. 건물의 예에서 볼 수 있드시 어떤 방식으로든지 누군가가 방어선 안으로

침투했다는 신호를 모니터할 수 있어야 합니다. 일반적으로 침입을 방지하는 것보다 침입으로부터 복구하는 것이 훨씬 더 피해가 크고 비용도 많이 듭니다.

방화벽의 경우, 최상의 전략은 테스트를 통해 신뢰할 수 있는 어플리케이션만 허용하는 것입니다. 이 전략을 위해서는 방화벽에서 실행할 서비스의 리스트를 철저히 정의해야 합니다. 연결 방향(내부에서 외부로 또는 외부에서 내부로)에 따라 각 서비스를 특징 지울 수 있습니다. 또한 각 서비스의 사용 권한을 부여할 사용자와 그 서비스를 위한 연결을 시작할 수 있는 기계도 나열해야 합니다.

네트워크 보호를 위해 방화벽이 할 수 있는 일

방화벽은 네트워크와 인터넷(또는 기타 신뢰할 수 없는 네트워크)의 연결 지점 사이에 설치하십시오. 이렇게 하면 방화벽을 사용하여 네트워크로의 진입점을 제한할 수 있습니다. 방화벽은 네트워크와 인터넷 사이에 하나의 연결점(초크점이라고 함)을 제공합니다(아래의 그림 참조). 연결점이 하나이기 때문에 네트워크로 들어가거나 나가는 통신을 더 잘 제어할 수 있습니다.

방화벽은 공용 네트워크에 하나의 주소로 나타납니다. 방화벽은 내부 네트워크 주소를 숨기는 동시에 프록시 서버, SOCKS 서버 또는 NAT(네트워크 주소 변환)를 통해 신뢰할 수 없는 네트워크에 대한 액세스를 제공합니다. 따라서 방화벽은 내부 네트워크 자체의 정보를 기밀로 유지시켜 줍니다. 네트워크 자체에 관한 정보를 유지하는 것이 방화벽에서 가장 공격(거짓)이 덜 발생하게 하는 방법입니다.

방화벽을 사용하면 네트워크로 들어가거나 나오는 통신을 제어하여 네트워크에 대한 공격 위험을 최소화할 수 있습니다. 방화벽은 네트워크로 들어가는 모든 통신을 안전하게 필터링함으로써 특정 목적지에 대해 특정 유형의 통신만 들어가도록 합니다. 따라서 누군가가 TELNET이나 FTP를 사용해서 내부 시스템에 액세스할 수 있는 위험을 최소화시킵니다.

네트워크 보호를 위해 방화벽이 할 수 없는 일

방화벽이 특정한 종류의 공격으로부터 상당한 보호를 제공하기는 하지만 전체 보안 솔루션의 일부에 지나지 않습니다. 예를 들어, 방화벽이 반드시 SMTP 메일, FTP 및 TELNET과 같은 어플리케이션을 통해 인터넷 상에서 송신되는 자료를 보호하는 것은 아닙니다. 이 자료를 암호화하도록 결정하지 않으면 자료가 목적지로 이동할 때 누구든지 인터넷에서 자료에 액세스할 수 있습니다.

iSeries 패킷 규칙

iSeries 400 패킷 규칙은 Operations Navigator 인터페이스에서 사용할 수 있는 OS/400의 통합 피처입니다. 패킷 규칙 피처를 사용하여 TCP/IP 통신 흐름을 제어하는 다음과 같은 두 가지의 핵심 네트워크 보안 기술을 구성함으로써 iSeries 시스템을 보호할 수 있습니다.

- 네트워크 주소 변환(NAT)
- IP 패킷 필터링

NAT와 IP 필터링이 OS/400의 한 부분으로 통합되어 있으므로 시스템 보안을 위한 경제적인 방법으로 사용할 수 있습니다. 경우에 따라서는 이 보안 방법이 추가 구매없이도 사용자가 필요로 하는 모든 것을 제공합니다. 그러나 이 방법으로는 실제적으로 기능하는 방화벽을 작성할 수 없습니다. 귀사의 보안 요구와 목표에 따라 IP 패킷 보안만 사용할 수도 있고 방화벽과 함께 사용할 수도 있습니다.

주: iSeries 생산 시스템을 보안할 계획이면, 경비 절감을 우선 원칙으로 고려해서는 안됩니다. 이와 같은 상황에서는 시스템 보안을 최우선 고려 대상으로 삼아야 합니다. 생산 시스템에 대한 최대한의 보호를 위해 방화벽의 사용을 고려하십시오.

NAT 및 IP 패킷 필터링의 정의 및 상호 작업 방식

네트워크 주소 변환(NAT)은 시스템을 통해 흐르는 패킷의 소스 또는 목적지 IP 주소를 변경합니다. NAT는 방화벽의 프록시 및 SOCKS 서버에 대해 보다 투명한 대안을 제공합니다. NAT는 또한 호환되지 않는 주소지정 구조의 네트워크들을 서로 연결시킴으로써 네트워크 구성을 단순화합니다. 따라서 주소지정 체계가 상충되거나 호환되지 않는 두 네트워크 사이에서 iSeries 시스템을 게이트웨이로 작동하기 위해 NAT 규칙을 사용할 수 있습니다. 또한 NAT를 사용하여 실제 IP 주소에 대해 하나 이상의 주소를 동적으로 대체하여 한 네트워크의 실제 IP 주소를 숨길 수 있습니다. IP 패킷 필터링과 NAT가 서로를 보완하므로, 네트워크 보안을 향상시키기 위해 함께 사용할 수도 있습니다.

NAT를 사용함으로써 방화벽 뒤에서 공용 웹 서버를 더 쉽게 조작할 수 있습니다. 즉, 웹 서버에 대한 공용 IP 주소를 개인용 내부 IP 주소로 변환합니다. 이것은 필요한 IP 주소의 등록 갯수를 줄여주며 기존 네트워크에 대한 충격을 최소화합니다. 또한 개인용 내부 IP 주소를 숨기는 반면에 내부 사용자가 인터넷에 액세스하기 위한 메카니즘을 제공합니다.

IP 패킷 필터링은 패킷 헤더에 있는 정보를 기초로 IP 통신을 선택적으로 차단하거나 보호하는 기능을 제공합니다. Operations Navigator에서 인터넷 설치 마법사를 통해 기본 필터링 규칙을 빠르고 쉽게 구성하여 불필요한 네트워크 통신을 막을 수 있습니다.

다음과 같은 작업에 IP 패킷 필터링을 사용할 수 있습니다.

- 사용자 네트워크에 허용할 IP 패킷과 네트워크로의 액세스를 거부할 IP 패킷을 지정하기 위해 필터 규칙 세트를 작성할 수 있습니다. 필터 규칙을 작성할 때, 필터 규칙을 실제 인터페이스(예: 토큰 링이나 이더넷 회선)에 적용하십시오. 여러 개의 실제 인터페이스에 규칙을 적용하거나 각 인터페이스에 서로 다른 규칙을 적용할 수 있습니다.

- 다음 헤더 정보를 기초로 특정 패킷을 허용하거나 거부하기 위한 규칙을 작성할 수 있습니다.
  - 목적지 IP 주소
  - 소스 IP 주소 프로토콜(예: TCP, UDP 등)
  - 목적지 포트(예: HTTP의 경우 포트 80)
  - 소스 포트
  - IP 데이터그램 방향(인바운드 또는 아웃바운드)
  - 이송(forward) 또는 로컬
- 원하지 않거나 불필요한 통신이 시스템의 어플리케이션에 도달하지 못하게 합니다. 또한 통신이 다른 시스템으로 이송되는 것을 막을 수 있습니다. 이것은 특정 어플리케이션 서버가 필요없는 하위 레벨 ICMP 패킷(예: PING 패킷)을 포함하고 있습니다.
- 필터 규칙이 시스템 저널의 규칙과 일치하는 패킷에 관한 정보를 가진 기록부 항목을 작성하는지 여부를 지정할 수 있습니다. 일단 정보가 시스템 저널에 기록되면, 그 기록부 항목을 변경할 수 없습니다. 결과적으로, 기록부가 네트워크 활동을 감사하기 위한 이상적인 툴입니다.

iSeries 네트워크 보안 옵션 선택

일반적으로, 권한이 없는 액세스로부터 보호하는 네트워크 보안 솔루션은 방화벽 기술에 기초하여 보호를 제공합니다. iSeries 400 시스템을 보호하기 위해 전기능 방화벽 제품을 사용하거나 특정 네트워크 보안 기술을 OS/400 TCP/IP 구현의 일부로 적용할 수 있습니다. 이와 같은 구현은 패킷 규칙 피처(IP 필터링과 NAT 포함)와 iSeries용 HTTP 프록시 서버 피처로 구성됩니다.

패킷 규칙 피처나 방화벽을 사용하는 것은 네트워크 환경, 액세스 요구사항 및 보안 요구에 의해 결정됩니다. iSeries 시스템이나 내부 네트워크를 인터넷이나 기타 신뢰할 수 없는 네트워크에 연결할 때마다 방화벽 제품을 기본 방어 장치로 사용하는 문제를 적극 고려해야 합니다.

대개는 방화벽이 외부 액세스를 위해 제한된 수의 인터페이스를 사용하는 전용 하드웨어와 소프트웨어 장치이기 때문에 이 경우에는 방화벽이 선호됩니다. 현재 사용 중인 인터넷 액세스 보호에 OS/400 TCP/IP 기술을 사용할 경우에는 무수한 인터페이스와 어플리케이션이 있는 범용 컴퓨팅 플랫폼이 외부 액세스에 개방됩니다.

이에 따른 차이점 여러 가지 이유에서 중요합니다. 예를 들어 전용 방화벽 제품은 방화벽 자체를 구성하는 것 이상의 다른 기능이나 어플리케이션을 제공하지 않습니다. 따라서 공격자가 방화벽을 성공적으로 우회하여 방화벽에 액세스하더라도 거의 수행할 수 있는 것이 없습니다. 그러나 공격자가 iSeries에서 TCP/IP 보안 기능을 성공적으로 우회할 경우 여러 가지의 유용한 어플리케이션, 서비스 및 자료에 액세스할 수 있게 됩니다. 따라서 공격자가 시스템 자체를 파괴하거나 내부 네트워크의 다른 시스템에 액세스할 수 있습니다.

그렇다면 iSeries TCP/IP 보안 피처를 언제까지나 허용할 수 있을까요? 선택한 다른 모든 보안 수단과 마찬가지로 비용과 이익 간의 득실을 기초로 의사를 결정해야 할 것입니다. 궁극적으로는 사업 목표를 분석하여 허용할 수 있는 위험 요소와 이와 같은 위험 요소를 최소화하기 위한 보안을 제공할 때 요구되는 비용을 비교하여 결정해야 합니다. 다음 표는 TCP/IP 보안 피처와 전기능 방화벽 장치를 비교하여 사용해야 할 시기에 관한 정보를 제공합니다. 이 표는 네트워크와 시스템 보호를 제공할 때 방화벽을 사용해야 하는지 또는 TCP/IP 보안 피처를 사용해야 하는지 아니면 그 둘을 함께 사용해야 하는지를 판별하는 데 도움이 됩니다.

보안 기술	**OS/400 TCP/IP** 기술 사용에 최적	전기능 방화벽 사용에 최적
IP 패킷 필터링	• 공용 웹 서버나 민감한 자료가 있는 인트라넷 시스템과 같은 단일 iSeries 시스템에 **추가** 보호를 제공하기 위해. • iSeries 시스템이 네트워크의 나머지 네트워크에 대한 게이트웨이(임시 라우터) 역할을 할 때 회사 **인트라넷**의 서브네트워크를 보호하기 위해. • iSeries 시스템이 게이트웨이 역할을 하는 **사설망** 또는 엑스트라넷 상에서 일정 수준에서 신뢰할 수 있는 상대방과의 통신을 제어하기 위해.	• 네트워크가 연결된 **인터넷**이나 기타 신뢰할 수 없는 네트워크로부터 전체 회사 네트워크를 보호하기 위해. • 회사 네트워크의 나머지로부터 통신량이 많은 큰 서브네트워크를 보호하기 위해.
네트워크 주소 변환 (NAT)	• 호환되지 않는 주소지정 구조를 가진 두 개의 **사설망** 연결을 작동시키기 위해. • 거의 신뢰할 수 없는 네트워크로부터 서브네트워크의 주소를 숨기기 위해.	• **인터넷**이나 기타 신뢰할 수 없는 네트워크에 액세스하는 클라이언트의 주소를 숨기기 위해. 프록시 서버와 SOCKS 서버의 대안으로 사용하기 위해. • 개인 네트워크의 시스템 서비스를 **인터넷**의 클라이언트가 사용할 수 있도록 하기 위해.
프록시 서버	• 중앙의 방화벽이 인터넷에 대한 액세스를 제공할 때 회사 네트워크의 **리모트 위치**에서 프록시 역할을 하기 위해.	• **인터넷**에 액세스할 때 전체 회사 네트워크의 프록시 역할을 하기 위해.

OS/400 TCP/IP 보안 피처의 사용 방법에 대한 자세한 정보는 다음 자원을 참조하십시오.

- 패킷 규칙(필터링 및 NAT)
- HTTP Server Documentation Center.
- AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

제 7 장 어플리케이션 보안 옵션

어플리케이션 레벨 보안 수단은 사용자들이 특정 어플리케이션과 대화하는 방법을 제어합니다. 일반적으로, 사용하는 각 어플리케이션에 대해 보안 설정을 구성해야 합니다. 그러나 인터넷으로부터 사용하거나 인터넷에 제공하려는 어플리케이션과 서비스에 대해서는 보안 설정에 특별히 주의해야 합니다. 이와 같은 어플리케이션과 서비스는 사용자의 네트워크 시스템에 액세스하기 위해 방법을 찾고 있는 권한이 없는 사용자의 오용에 매우 취약합니다. 사용할 보안 수단은 서버쪽 보안 노출 요소와 클라이언트쪽 보안 노출 요소를 모두 포함하는 것이어야 합니다.

사용할 각 어플리케이션의 보안도 중요하지만 전체적인 보안 정책을 구현함에 있어서 보안 수단 또한 하나의 작은 부분을 차지합니다. 따라서 보안 수단을 적용해야 합니다.

일반적인 여러 인터넷 어플리케이션 보안에 대해 자세히 알려면 다음 페이지를 검토하십시오.

- 『웹 제공 보안』
- 31 페이지의 『Java 인터넷 보안』
- 34 페이지의 『전자 우편 보안』
- 35 페이지의 『FTP 보안』

웹 제공 보안

방문자에게 자신의 웹 사이트에 대한 액세스를 제공할 때, 사이트 구성 방법 및 페이지 생성에 사용한 코딩 관련 정보가 노출되는 것을 원하지 않을 것입니다. 또한 방문자들이 보게 될 화면의 뒤에서 이루어지는 모든 작업들을 포함하여 모든 페이지를 쉽고 빠르게 그리고 막힘없이 볼 수 있기를 원할 것입니다. 관리자로서 귀하는 보안 방침이 웹 사이트에 부정적인 영향을 주지 않기를 원할 것입니다. iSeries 400을 웹 서버로 사용할 때는 다음 사항을 고려하십시오.

- 클라이언트가 HTTP 서버와 대화하기 전에 서버 관리자가 서버에 대한 지시문을 정의해야 합니다. 보안 검사를 작성하기 위한 방법에는 일반 서버 지시문과 서버 보호 지시문의 두 가지가 있습니다. 서버가 요청을 받아들이기 전에 웹 서버에 대한 요청이 이 지시문에서 제공하는 모든 제한사항을 충족시켜야 합니다.
- 서버 구성을 위한 서버 관리 웹 페이지를 사용하여 이 지시문을 작성하고 편집할 수 있습니다. 서버 지시문을 통해 웹 서버의 전반적인 작동을 제어할 수 있습니다. 또한 서버 보호 지시문을 통해 웹 서버가 처리하는 특정 URL을 위해 서버가 사용하는 보안 모델을 지정 및 제어할 수 있습니다.
- 서버를 구성하기 위해 map 또는 pass 지시문과 서버 관리 웹 페이지를 사용할 수 있습니다.

– map이나 pass 지시어를 사용하여 파일명을 iSeries 웹 서버에 표시해야 합니다. 자세히 설명하면, URL을 제공하는 웹 서버의 지시문을 제어하기 위한 PASS 서버 지시문과 MAP 서버 지시문이 있습니다. 또한 CGI-BIN 프로그램이 상주하는 라이브러리를 제어하기 위한 EXEC 서버 지시문도 있습니다.

  각 서버 URL을 위한 보호 지시문을 정의하십시오. 모든 URL에 보호 지시문이 필요한 것은 아닙니다. 그러나 URL 자원의 액세스 방법이나 액세스하는 사람을 제어하기 하려는 경우, 해당 URL에 대한 보호 지시문이 반드시 필요합니다.
– 또한 WRKHTTPCFG(HTTP 구성에 대한 작업 명령)를 사용하고 지시문을 입력하는 대신 서버를 구성하기 위해 서버 관리 웹 페이지를 사용할 수 있습니다. 명령 행 인터페이스를 통해 보호 지시문에 대해 작업하는 것은 매우 복잡할 수 있습니다. 그러므로 지시문을 올바르게 설정하기 위해서는 관리 웹 페이지를 사용하는 것이 좋습니다.

HTTP는 데이터베이스 파일에 있는 자료를 표시는 하되 수정은 할 수 없는 기능을 제공합니다. 그러나 데이터베이스 파일을 갱신하기 위해 사용자가 작성해야 하는 일부 어플리케이션이 있습니다. 이 경우 CGI-BIN 프로그램을 사용할 수 있습니다. 예를 들어, 사용자가 양식을 작성하여 완성한 후에 iSeries 데이터베이스를 갱신할 수 있습니다. 보안 관리자로서 귀하는 그 사용자 프로파일의 권한 부여 상태와 CGI 프로그램이 수행하는 기능을 모니터해야 합니다. 또한 민감한 오브젝트가 부적절한 공용 권한을 가질 수 있는 가능성에 대해서도 반드시 평가해야 합니다.

주: 공통 게이트웨이 인터페이스(CGI)는 웹 서버와 그 외부의 컴퓨터 프로그램 사이에서 정보를 교환하기 위한 업계 표준입니다. 웹 서버가 실행되는 오퍼레이팅 시스템에서 지원하는 어떠한 프로그래밍 언어로나 프로그램을 작성할 수 있습니다.

웹 페이지에서 CGI 프로그램을 사용하는 것과 함께 Java를 원할 경우가 있습니다. 웹 페이지에 Java를 추가하려면 먼저 Java 보안의 내용을 이해해야 합니다.

HTTP 서버는 서버를 통해 이루어진 액세스와 시도된 액세스를 둘다 모니터하는 데 사용할 수 있는 액세스 기록부를 제공합니다.

프록시 서버는 웹 서버로부터 HTTP 요청을 수신하여 웹 서버로 다시 송신합니다. 이 요구를 수신하는 웹 서버는 프록시 서버 IP 주소만을 인식합니다. 웹 서버는 요구를 시작한 PC의 이름이나 주소를 판별할 수 없습니다. 프록시 서버는 HTTP, FTP(파일 전송 프로토콜), Gopher 및 WAIS용 URL 요구를 처리할 수 있습니다.

iSeries용 IBM HTTP Server의 HTTP 프록시 지원을 사용하여 웹 액세스를 통합할 수도 있습니다.  프록시 서버는 또한 추적 목적을 위해 모든 URL 요구를 기록할 수 있습니다. 따라서 기록부를 검토하여 네트워크 자원의 사용과 오용을 모니터할 수 있습니다.

이 주제에 관한 자세한 정보는 *iSeries 보안을 위한 추가 정보 및 툴을 참조하십시오* 

Java 인터넷 보안

근래에는 Java 프로그래밍이 컴퓨팅 환경에 점차 확산되어 가고 있습니다. 예를 들어, 새로운 어플리케이션을 개발하기 위해 시스템에서 IBM Toolbox for Java 또는 IBM Development Kit for Java를 사용할 수 있습니다. 결과적으로, Java와 연관되는 보안 문제를 처리할 준비를 갖추어야 합니다. 방화벽이 인터넷 보안 위험을 방어하는 가장 일반적인 장치라고는 하지만 Java를 사용함으로 인해 발생할 수 있는 다른 많은 위험 요소에 대해서는 보호를 제공하지 않습니다. 보안 정책에는 Java에 중요한 세 영역, 즉 어플리케이션, 애플릿, 서브릿으로부터 시스템을 보호하는 세부사항을 포함시켜야 합니다. 또한 Java 프로그램에 대한 인증 및 권한 부여와 관련하여 Java와 자원 보안의 상호작용에 대해서도 이해해야 합니다.

Java 어플리케이션

하나의 언어로서 Java에는 무결성 문제점을 유발할 수 있는 예기치 않은 오류로부터 Java 프로그래머를 보호하는 특성이 있습니다. (C 또는 C++과 같이 PC 어플리케이션에 일반적으로 사용되는 다른 언어는 Java처럼 예기치 않은 오류로부터 프로그래머를 강력히 보호해주지 않습니다.) 예를 들어, Java는 프로그래머가 의도하지 않은 방법으로 오브젝트를 사용하지 못하도록 보호하는 강한 형(strong typing)을 사용합니다. Java는 포인터 조작을 허용하지 않음으로써 프로그래머가 우발적으로 프로그램의 메모리 경계 밖으로 나가지 못하도록 보호합니다. 어플리케이션 개발 관점에서, 사용자들은 Java를 다른 고급 언어를 보는 것처럼 볼 수 있습니다. iSeries 400에서 다른 언어에 적용하는 것과 동일한 보안 규칙을 어플리케이션 설계에 적용해야 합니다.

Java 애플릿

Java 애플릿은 HTML 페이지에 포함시킬 수 있는 작은 Java 프로그램입니다. 애플릿이 클라이언트에서 실행되기 때문에, 애플릿이 수행하는 것은 클라이언트에 관한 것입니다. 그러나 Java 애플릿은 iSeries 400에 액세스할 수 있습니다. (네트워크의 PC에서 작동하는 ODBC 프로그램이나 APPC(advanced program-to-program communication) 프로그램도 iSeries에 액세스할 수 있습니다.) 일반적으로 Java 애플릿은 애플릿이 시작된 서버와만 세션을 설정할 수 있습니다. 따라서, Java 애플릿은 iSeries(예: 웹 서버)의 애플릿일 때만 연결된 PC에서 iSeries에 액세스할 수 있습니다.

애플릿은 서버의 어느 TCP/IP 포트에나 연결을 시도할 수 있습니다. Java로 작성된 소프트웨어 서버의 경우도 물론 해당됩니다. 그러나 IBM Toolbox for Java를 사용하여 서버를 작성한 경우, 서버로의 연결을 다시 설정할 때 애플릿이 사용자 ID와 암호를 제공해야 합니다. 본 정보에서 설명하고 있는 모든 서버는 iSeries 서버입니다. (Java로 작

성한 서버는 IBM Toolbox for Java를 사용하지 않아도 됩니다.) 일반적으로, IBM Toolbox for Java 클래스의 경우에는 첫 번째 연결에서 사용자가 사용자 ID와 암호를 입력할 것을 요구받습니다.

애플릿은 사용자 프로파일이 해당 기능에 대한 권한을 가지고 있는 경우에만 iSeries 시스템에서 기능을 수행할 수 있습니다. 그러므로 새로운 어플리케이션 기능을 제공하기 위해 Java 애플릿을 사용할 때는 훌륭한 자원 보안 체계가 필수적입니다. 시스템이 애플릿으로부터의 요구를 처리할 때, 시스템은 사용자 프로파일에 있는 제한 성능 값을 사용하지 않습니다.

애플릿 표시기는 서버 시스템에서 애플릿을 테스트할 수 있게 해 주지만, 브라우저 보안 제한사항에 따라 결정되는 것이 아닙니다. 따라서 사용자의 애플릿을 테스트하기 위해서만 애플릿 표시기를 사용해야 하며, 외부 자원으로부터 애플릿을 실행하기 위해 사용해서는 안됩니다. 때로는 Java 애플릿이 사용자의 PC 드라이브에 작성되기도 하며 이로 인해 애플릿이 파괴적 조치를 수행할 가능성이 있습니다. 그러나 인증을 위해 Java 애플릿에 서명할 때 디지털 인증을 사용할 수 있습니다. 서명된 애플릿(signed applet)은 브라우저에 대한 디폴트 설정값이 PC의 로컬 드라이브에 작성하는 것을 금지하더라도 작성할 수 있습니다. 또한 iSeries에서 맵핑된 드라이브가 PC에서는 로컬 드라이브로 나타나기 때문에 맵핑된 드라이브에도 서명된 애플릿을 작성할 수 있습니다.

주: 일반적으로 Netscape Navigator와 MS Internet Explorer의 경우에는 위에서 설명한 작동 방식이 해당됩니다. 실제로 발생하는 사항은 사용하는 브라우저의 구성과 관리 방법에 따라 다릅니다.

iSeries에서 시작된 Java 애플릿의 경우에는 서명된 애플릿을 사용해야 합니다. 그러나 사용자들에게 통지하여 일반적으로 알 수 없는 소스에서 서명된 애플릿은 허용하지 않도록 해야 합니다.

V4R4부터는 IBM Toolbox for Java를 사용하여 SSL 환경을 설정할 수 있습니다. 또한 IBM Developer Toolkit for Java를 사용하여 SSL로 Java 어플리케이션을 보안할 수도 있습니다. Java 어플리케이션에 SSL을 사용하면 클라이언트와 서버 사이를 통과하는 사용자 ID와 암호를 포함하여 자료가 암호화됩니다. 등록된 Java 프로그램을 구성하여 SSL을 사용하려는 경우, 디지털 인증 관리자를 사용할 수 있습니다.

Java 서브릿

서브릿은 Java로 작성된 서버 구성요소로서, 웹 서버 코드를 변경하지 않고도 웹 서버의 기능을 동적으로 확장합니다. iSeries용 IBM HTTP Server와 함께 제공되는 IBM WebSphere 어플리케이션 서버는 iSeries 시스템에서 서브릿을 사용하기 위한 지원을 제공합니다.

반드시 서버가 사용하는 서브릿 오브젝트에 자원 보안을 사용해야 합니다. 그러나 자원 보안을 서브릿에 적용하는 것만으로 충분히 안전한 것은 아닙니다. 일단 웹 서버가 서

브릿을 로드한 후에는 자원 보안이 더 이상 다른 자원이 해당 서브릿을 실행하는 것을 막지 않습니다. 따라서 HTTP Server 보안 제어와 지시문을 포함하여 자원 보안도 사용해야 합니다. 예를 들어, 서브릿이 웹 서버의 프로파일로만 실행되지 않도록 하십시오. 그 외에도 HTTP 서버 그룹과 액세스 제어 리스트(ACL)를 사용하여 서브릿(보호 지시문의 마스크 키워드)을 실행할 수 있는 사람을 제어해야 합니다. 또한 iSeries용 WebSphere Application Server에 있는 보안 피처와 같이 서브릿 개발 툴에서 제공하는 보안 피처를 사용해야 합니다.

Java를 위한 일반적인 보안 수단에 관해 자세히 알려면 다음 정보를 검토하십시오.
- IBM Developer Kit for Java Java 보안
- IBM Toolbox for Java 보안 클래스
- iSeries 보안을 위한 추가 정보 및 툴 

자원에 대한 Java 인증 및 권한 부여

IBM Toolbox for Java 안에는 사용자 ID를 확인하고, iSeries 시스템에서 실행되는 어플리케이션이나 서브릿의 오퍼레이팅 시스템 스레드에 ID를 선택적으로 할당하는 보안 클래스가 들어 있습니다. 자원 보안을 위한 후속 검사는 할당된 ID에서 발생합니다. 이 보안 클래스에 대한 자세한 내용은 IBM Toolbox for Java 인증 서비스를 참조하십시오.

IBM Developer Kit for Java는 J2SDK(Java 2 Software Development Kit) 표준 버전의 표준 확장판인 Java 인증 및 권한 부여 서비스(JAAS)에 대한 지원을 제공합니다. 현재 J2SDK는 코드가 시작된 장소와 코드를 서명한 사람(코드 소스 기반 액세스 제어)을 기준으로 액세스 제어를 제공합니다. J2SDK 사용에 대한 자세한 내용은 Java 인증 및 권한 부여 서비스 및

SSL을 사용한 Java 어플리케이션 보안

SSL을 사용하여 IBM Developer Kit for Java로 개발한 iSeries 어플리케이션의 통신을 보안할 수 있습니다. IBM Toolbox for Java를 사용하는 클라이언트 어플리케이션도 SSL을 활용할 수 있습니다. 사용자 소유의 Java 어플리케이션을 위해 SSL을 작동 가능하게 만드는 프로세스는 다른 어플리케이션을 위한 프로세스와 약간 다릅니다.

Java 어플리케이션의 보안 소켓층 관리에 대한 자세한 정보는 Information Center에서 다음 주제를 참조하십시오.
- IBM Toolbox for Java 보안 소켓층(SSL) 환경.
- SSL을 사용하여 Java 어플리케이션을 보안하는 IBM Developer Toolkit for Java.

전자 우편 보안

인터넷이나 기타 신뢰할 수 없는 네트워크에서의 전자 우편을 사용하는 것은 방화벽으로 보호할 수 없는 보안 위험 요소를 노출시킵니다. 보안 정책에 이러한 위험을 최소화하는 방법을 확실히 설명하기 위해서는 이와 같은 위험 요소를 잘 알아야 합니다.

전자 우편은 또 다른 형태의 통신으로 볼 수 있습니다. 전자 우편을 통해 기밀 정보를 송신할 때는 세심한 주의가 필요합니다. 전자 우편은 수신 전에 많은 서버를 지나기 때문에 누군가 가로채서 읽을 수 있습니다. 따라서 보안 수단을 사용하여 전자 우편의 기밀성을 보호해야 할 것입니다.

전자 우편의 일반적인 보안 위험 요소

전자 우편 사용과 관련하여 몇 가지 위험 요소가 있습니다.

- **넘침**(서비스 거부 공격 유형의 하나)은 시스템이 많은 수의 전자 우편 메세지로 과부하 상태가 될 때 발생합니다. 공격자가 많은 전자 우편 메세지(빈 메세지 포함)를 하나의 전자 우편 서버로 송신해서 서버를 넘치게 하는 프로그램을 작성하기는 비교적 쉽습니다. 서버의 저장 디스크가 불필요한 메세지로 채워지기 때문에 적절한 보안이 없으면 목표 서버에 서버의 거부가 발생할 수 있습니다. 또는 모든 서버 자원이 공격으로 인한 메일 처리에 관여하므로 서버가 응답을 중단합니다.
- **스팸**(정크 메일)은 전자 우편에서 일반적으로 발생하는 또 다른 공격 유형입니다. 인터넷을 통해 e-commerce를 제공하는 업체 수가 증가함에 따라, 사업과 관련된 전자 우편에 있어서 자신이 원하지 않거나 요청하지 않은 전자 우편의 폭발적 증가를 이미 경험하고 있습니다. 이것은 정크 메일로서, 전자 우편 사용자의 광범위한 분배 리스트에 송신되어 각 사용자의 전자 우편함을 채웁니다.
- **기밀성(Confidentiality)**은 인터넷을 통해 다른 사람에세 전자 우편이 송신되는 것과 연관된 위험입니다. 이 전자 우편은 자신이 지정한 수신자에게 도달하기 전에 많은 서버를 통과합니다. 따라서 메세지를 암호화하지 않으면 해커가 전달 경로의 어느 곳에서나 사용자의 메일을 선택하여 읽을 수 있습니다.

전자 우편 보안 옵션

넘침과 스팸 위험으로부터 보호하려면 반드시 전자 우편 서버를 올바로 구성해야 합니다. 대부분의 서버 어플리케이션들은 이와 같은 유형의 공격을 처리하는 메소드를 제공합니다. 또한 ISP가 이와 같은 공격에 대해 몇 가지 추가 보호를 제공할 수 있도록 ISP와 함께 작업할 수 있습니다.

필요한 추가 보안 수단은 전자 우편 어플리케이션이 제공하는 보안 피처 뿐만 아니라 필요한 기밀성 레벨에 따라서 다릅니다. 예를 들어, 전자 우편 메세지의 내용이 충분히 기밀 상태를 유지하는지 또는 발신지나 목표 IP 주소와 같이 전자 우편과 관련된 모든 정보를 비밀로 유지할 것인지 등입니다.

일부 어플리케이션들은 사용자에게 필요한 보호를 제공하는 통합 보안 피처를 가지고 있습니다. 예를 들어, Lotus NotesDomino™는 문서 전체나 문서의 개별 필드에 대한 암호화 기능을 포함하여 여러 가지 통합 보안 피처를 제공합니다.

메일을 암호화하기 위해서 Lotus Notes Domino는 사용자별로 고유한 공용 키 및 개인 키를 작성합니다. 공용 키를 가진 사용자만 메세지를 읽을 수 있도록 메세지를 암호화하는 데 개인 키가 사용됩니다. 반드시 지정한 노트 수신자에게 공용 키를 송신하여 그 키를 사용하여 암호화된 노트를 해독할 수 있게 해야 합니다. 누군가 암호화된 메일을 송신하면 Lotus Notes Domino는 송신자의 공용 키를 사용하여 노트를 해독합니다.

Notes 암호화 피처 사용에 대한 내용은 프로그램의 온라인 도움말 파일에 있습니다.

iSeries에서의 Domino™ 보안에 대한 자세한 내용은 다음 참조서를 참조하십시오.

- Lotus Domino reference library
- Lotus Notes user assistance 웹 사이트
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed (SG24-5341)
- Lotus Domino for AS/400 Internet Mail and More (SG24-5990)

지사, 리모트 클라이언트, 사업 상대 사이에서 흐르는 전자 우편이나 기타 정보에 기밀성을 제공할 때 몇 가지 옵션을 사용할 수 있습니다.

전자 우편 서버 어플리케이션이 SSL(보안 소켓층)을 지원하는 경우, SSL을 사용하여 서버와 전자 우편 클라이언트 사이에 보안 통신 세션을 작성할 수 있습니다. SSL은 클라이언트쪽 인증을 사용하기 위해 클라이언트 어플리케이션이 작성될 때 클라이언트쪽 인증(선택적)에 대한 지원도 제공합니다. 전체 세션이 암호화되므로 SSL도 자료 전송 중에 자료 무결성을 유지합니다.

사용할 수 있는 또다른 옵션은 VPN(가상 사설망) 연결을 구성하는 것입니다. V4R4부터는 iSeries를 사용하여 리모트 클라이언트와 iSeries 시스템을 포함한 여러 VPN 연결을 구성할 수 있습니다. VPN을 사용하면 통신 종료점 사이의 모든 통신이 암호화되어 자료 기밀성과 자료 무결성이 모두 유지됩니다.

FTP 보안

파일 전송 프로토콜(FTP)은 클라이언트(다른 시스템의 사용자)와 서버 사이에 파일 전송 기능을 제공합니다. 또한 리모트 명령 기능을 사용하여 서버에 명령을 제출할 수도 있습니다. 따라서 FTP는 리모트 시스템에서 작업하거나 시스템 간에 파일을 이동할 때 매우 유용합니다. 그러나 인터넷이나 신뢰할 수 없는 기타 네트워크에서 FTP를 사용하

는 것은 사용자를 특정 보안 위험에 노출시키는 결과를 가져옵니다. 이러한 위험 요소를 파악해서 위험을 최소화하는 방법을 보안 정책에 설명하도록 해야 합니다.

- 시스템에서 FTP를 허용할 때 사용자의 오브젝트 권한 체계가 충분한 보호를 제공하지 않을 수 있습니다.

  예를 들어, 사용자 오브젝트에 대한 공용 권한이 *USE일 수 있으나 현재로는 "메뉴 보안"을 사용하여 대부분의 사용자들이 그러한 오브젝트에 액세스하는 것을 막고 있습니다. (메뉴 보안은 메뉴 옵션에 포함된 것이 아니면 사용자들이 어떤 작업도 수행하지 못하게 합니다.) FTP 사용자들은 메뉴에 제한을 받지 않으므로, 시스템의 모든 오브젝트를 읽을 수 있습니다. 다음은 이와 같은 보안 위험을 제어하는 몇 가지 옵션입니다.

  - 시스템의 전체 iSeries 오브젝트 보안을 실행합니다(즉 시스템의 보안 모델을 "메뉴 보안"에서 "오브젝트 보안"으로 변경). 이것이 가장 안전한 최상의 옵션입니다.
  - FTP를 통해 전송될 수 있는 파일의 액세스를 제한하기 위해 FTP를 위한 나감 프로그램을 작성합니다. 나감 프로그램은 메뉴 프로그램이 제공하는 보안과 최소한 같은 수준의 보안을 제공합니다. 많은 고객들은 FTP 액세스 제어가 더욱 제한적이기를 원할 것입니다. 이 옵션은 ODBC, DDM 또는 DRDA와 같은 다른 인터페이스가 아닌 FTP만을 처리합니다.

    주: 파일에 대한 *USE 권한은 사용자들이 그 파일을 다운로드하는 것을 허용합니다. 파일에 대한 *CHANGE 권한은 사용자들이 그 파일을 업로드하는 것을 허용합니다.

- 해커가 FTP 서버로 "서비스 거부" 공격을 개시하여 시스템에서 사용자 프로파일이 작동하지 않게 만들 수 있습니다. 이것은 사용자 프로파일이 작동하지 않을 때까지 사용자 프로파일에 맞지 않는 암호로 여러 차례 로그온하는 경우에 발생합니다. 최대 3회까지 사인 온을 하게 되면 이런 유형의 공격으로 프로파일이 작동하지 않습니다.

  이와 같은 위험을 피하기 위해 할 수 있는 것으로는 공격을 최소화하기 위해 보안을 강화하는 것과 사용자들에게 쉬운 액세스를 제공하는 것 사이의 득실을 분석하는 일이 포함됩니다. FTP 서버는 일반적으로 QMAXSIGN 시스템 값을 적용함으로써 해커들이 암호를 추측하여 암호 공격을 무제한적으로 시도하지 못하게 합니다. 다음은 FTP를 사용할 때 고려해야 할 몇 가지 옵션입니다.

  - 시스템 사용자 프로파일과 FTP 액세스가 허용되지 않는 사용자 프로파일의 로그온 요청을 거부하기 위해 FTP 서버 로그온 나감 프로그램을 사용합니다. (그와 같은 나감 프로그램을 사용할 때, 사용자가 봉쇄시킨 사용자 프로파일의 서버 로그온 나감점이 거부한 로그온 시도는 프로파일의 QMAXSIGN 계수에 계산되지 **않습니다**.)
  - 해당 사용자 프로파일이 FTP 서버에 액세스할 수 있는 클라이언트 컴퓨터를 제한하기 위해 FTP 서버 로그온 나감 프로그램을 사용합니다. 예를 들어, 회계 부서의 한 사람에게 FTP 액세스가 허용된 경우, 회계 부서에서 IP 주소를 가진 컴퓨터로부터만 사용자 프로파일 FTP 서버 액세스를 허용하십시오.

– 모든 FTP 로그온을 시도하는 사용자명과 IP 주소를 기록하기 위해 FTP 서버 로그온 나감 프로그램을 사용하십시오. 이 기록부를 정기적으로 검토하여 프로파일이 최대 암호 시도 수로 인해 작동이 불가능해질 때마다 IP 주소 정보를 사용하여 침입자를 식별한 후 적절한 수단을 취하십시오.

그 외에도 FTP 서버 나감점을 사용하여 게스트 사용자에게 익명의 FTP 기능을 제공할 수 있습니다. 안전한, 익명의 FTP 서버를 설정하는 것은 FTP 서버 로그온 및 FTP 서버 요구 확인 나감점 모두에 있어서 나감 프로그램이 필수적입니다.

V5R1부터는 보안 소켓층(SSL)을 사용하여 FTP 서버에 안전한 통신 세션을 제공할 수 있습니다. SSL을 사용하면 모든 FTP 전송이 암호화되므로 사용자명과 암호를 포함하여 FTP 서버와 클라이언트 사이를 통과하는 모든 자료의 기밀성이 유지됩니다. FTP 서버는 클라이언트 인증을 위해 디지털 인증 사용도 지원합니다.

FTP 사용, 위험 요소 및 사용 가능한 보안 수단에 대한 자세한 내용은 다음 자원을 검토하십시오.

- FTP 보안 구현.
- 익명의 FTP.
- FTP 보안.
- iSeries 보안을 위한 추가 정보 및 툴  .

제 8 장 전송 보안 옵션

JKL Toy사 시나리오에는 두 개의 1차 iSeries 400 시스템이 있습니다. 회사는 하나를 개발용으로, 하나는 생산 어플리케이션용으로 사용합니다. 두 시스템 모두 업무에 중요한 자료와 어플리케이션을 처리합니다. 따라서, 회사에서는 인트라넷과 인터넷 어플리케이션을 처리하기 위해 주변 네트워크에 신규 iSeries 시스템을 추가하기로 결정했습니다.

주변 네트워크를 구축함으로써, 내부 네트워크와 인터넷을 물리적으로 분리할 수 있습니다. 이러한 분리는 내부 시스템이 취약한 면을 드러내는 인터넷 위험 요소들을 감소시킵니다. 또한 회사에서는 신규 iSeries 400을 인터넷 서버 전용으로 지정하여 네트워크 보안 관리의 복잡성을 줄였습니다.

인터넷 환경에 있어서 보안을 위한 퍼베이시브 요구로 인해, IBM은 인터넷에서 e-비즈니스를 수행하기 위해 보안 네트워킹 환경을 보장하는 보안 오퍼링을 계속적으로 개발하고 있습니다. 인터넷 환경에서는 시스템 고유 보안과 어플리케이션 고유 보안을 모두 제공해야 합니다. 그러나 회사 인트라넷이나 인터넷 연결을 통해 비밀 정보를 이동하기 위해서는 보다 강력한 보안 솔루션의 구현이 더욱 요구됩니다. 따라서 인터넷에서 자료 전송이 이루어지는 동안 자료 전송을 보호하는 보안 수단을 구현해야 합니다.

iSeries를 위한 두 가지의 고유한 전송 레벨 보안 오퍼링인 보안 소켓층(SSL) 보안 통신 및 VPN(가상 사설망) 연결을 이용하여 신뢰할 수 없는 시스템 간의 정보 이동과 관련된 위험을 최소화할 수 있습니다.

SSL을 사용한 어플리케이션 보안

보안 소켓층(SSL) 프로토콜은 클라이언트와 서버 사이의 통신을 보안하기 위한 업계 표준입니다. SSL은 원래 웹 브라우저 어플리케이션용으로 개발된 것이지만, 지금은 점점 더 많은 어플리케이션이 SSL을 사용하고 있습니다. iSeries의 경우, 다음과 같은 어플리케이션에서 SSL을 사용합니다.

- iSeries용 IBM HTTP Server(Apache로 구현)
- FTP 서버
- Telnet 서버
- 분산 관계형 데이터베이스 구조(DRDA) 및 분산 자료 관리
- (DDM) 서버
- 중앙 관리
- 디렉토리 서비스 서버(LDAP)

- Operations Navigator를 포함한 Client Access Express 어플리케이션 및 어플리케이션 프로그래밍 인터페이스(API)의 Client Access Express 세트로 작성된 어플리케이션
- Developer Kit for Java를 사용하여 개발한 프로그램 및 IBM Toolkit for Java를 사용하는 클라이언트 어플리케이션
- 어플리케이션에서 SSL을 작동하는 데 사용할 수 있는 보안 소켓층(SSL) 어플리케이션 프로그래밍 인터페이스(API)를 통해 개발한 프로그램. SSL을 사용하는 프로그램 작성법에 대한 자세한 정보는 보안 소켓층 API를 참조하십시오.

이와 같은 여러 어플리케이션은 또한 클라이언트 인증을 위한 디지털 인증 사용도 지원합니다. SSL은 통신 상대를 인증하고 보안 연결을 작성하는데 있어서 디지털 인증에 의존합니다.

iSeries VPN(가상 사설망)

iSeries 시스템 VPN 연결을 사용하여 두 종료점 사이에 보안 통신 채널을 설정할 수 있습니다. SSL 연결과 마찬가지로, 종료점 사이에서 이동하는 자료를 암호화할 수 있으므로, 자료 기밀성과 자료 무결성 모두가 제공됩니다. 그러나 VPN 연결은 사용자가 지정하는 종료점으로 통신 흐름을 제한함과 동시에 연결을 사용할 수 있는 통신 유형을 제한할 수 있게 해줍니다. 그러므로 VPN 연결은 권한이 없는 액세스로부터 네트워크 자원을 보호할 수 있도록 일정한 수준의 네트워크 레벨 보안을 제공합니다.

사용해야 할 방법

이러한 두 가지 보안 방법 모두 보안 인증, 자료 기밀성 및 자료 무결성에 대한 요구를 처리합니다. 어느 방법을 사용해야 할 것인지는 여러 요인에 의해 결정됩니다. 특별히 고려해야 할 요인으로는 통신 상대, 통신에 사용하는 어플리케이션, 통신 보안에 대한 비용과 성능의 균형 등입니다.

또한 SSL과 함께 특정 어플리케이션을 사용하려는 경우, 그 어플리케이션이 SSL을 사용할 수 있도록 반드시 설정되어 있어야 합니다. 많은 어플리케이션에서 아직 SSL의 장점을 이용할 수는 없지만, Telnet과 Client Access Express 등 기타 많은 어플리케이션에는 SSL 기능이 추가되었습니다. 그 외에도 VPN을 사용하면 특정 연결 종료점 사이를 흐르는 모든 IP 통신을 보호할 수 있습니다.

예를 들어, 현재 내부 네트워크에서 사업 상대가 웹 서버와 통신할 수 있도록 하기 위해 SSL에서 HTTP를 사용할 수 있습니다. 웹 서버가 사용자와 사업 상대 사이에 필요한 유일한 보안 어플리케이션이면, VPN 연결로 전환하기를 원하지 않을 것입니다. 그러나 통신을 확장하려 한다면, VPN 연결을 대신 사용할 수 있습니다. 또한 네트워크 일부의 통신을 보호해야 하지만 SSL을 사용하기 위해 각 클라이언트와 서버를 따로 구성할 수 없는 상황이 있을 수 있습니다. 네트워크의 해당 부분에 대해 게이트웨이 간에 VPN 연결을 작성할 수 있습니다. 이것이 해당 통신을 보안하는 한편 연결의 어느 한 쪽에 있는 개별 서버와 클라이언트에 대해 투명한 연결을 제공합니다.

SSL에 디지털 인증 사용

디지털 인증은 통신 보안을 위해 그리고 더 강력한 인증 수단으로서 보안 소켓층(SSL)을 사용하기 위한 기초를 제공합니다. iSeries 400은 OS/400의 통합 피처인 디지털 인증 관리자(DCM)를 사용하는 시스템과 사용자에게 디지털 인증을 쉽게 작성 및 관리할 수 있는 기능을 제공합니다.

또한 강력한 클라이언트 인증 메소드에 사용자명과 암호 대신, 디지털 인증을 사용하기 위해 iSeries용 IBM HTTP Server 등 일부 어플리케이션을 구성할 수 있습니다.

디지털 인증의 정의

디지털 인증이란 암호처럼 인증 소유자의 ID를 유효하게 만드는 디지털 증명서입니다. 이것은 **인증 기관(CA)**이라고 하는 신뢰할 수 있는 제3자가 서버와 사용자에게 디지털 인증을 발행합니다. CA에 있어서 신뢰라고 하는 것은 유효한 신임장과 같이 인증서에서 신뢰의 기본이 되는 것입니다.

CA마다 CA가 인증서를 발행하기 위해서 요구하는 식별 정보를 판별하기 위한 정책이 있습니다. 어떤 인터넷 CA에서는 식별명 정도의 매우 적은 양의 정보만 요구합니다. 이것이 CA가 디지털 인증 주소 및 디지털 전자 우편 주소를 발행할 사람이나 서버의 이름입니다. 개인 키와 공용 키가 각 인증서에 대해 생성됩니다. 인증서는 공용 키를 포함하고 있는 반면에 브라우저나 보안된 파일은 개인 키를 저장하고 있습니다. 인증서의 소유자가 이 키를 사용하여 메세지나 문서와 같이 사용자와 서버 사이에서 전송되는 자료를 ″서명″하고 암호화할 수 있습니다. 이러한 디지털 서명이 그 항목이 원본임을 보장함과 동시에 무결성을 보호합니다.

많은 어플리케이션에서 아직 SSL의 장점을 이용할 수는 없지만, Telnet과 Client Access Express 등 기타 많은 어플리케이션에는 SSL 기능이 추가되었습니다. iSeries 어플리케이션에서 SSL을 사용하는 방법에 관해서는 iSeries Information Center에서 **SSL을 사용한 어플리케이션 보안**을 참조하십시오.

Telnet 액세스 보안을 위한 SSL

현재 V4R4에서는 Telnet 통신 세션의 보안에 보안 소켓층(SSL)을 사용하도록 Telnet 서버를 구성할 수 있습니다. SSL을 사용하도록 Telnet 서버를 구성하기 위해서는 반드시 디지털 인증 관리자(DCM)를 사용하여 Telnet 서버의 인증을 구성해야 합니다. 디폴트로 Telnet 서버는 보안 및 비보안 연결 모두를 처리합니다. 그러나 보안 Telnet 세션만 허용하도록 Telnet을 구성할 수 있습니다. 또한 더 강력한 클라이언트 인증을 위해 디지털 인증을 사용하도록 Telnet 서버를 구성할 수도 있습니다.

Telnet과 함께 SSL을 사용하도록 선택하면 강력한 보안 처리에 따른 여러 가지 이점이 있습니다. Telnet의 경우, 서버 인증과는 별도로 Telnet 프로토콜 자료 흐름에 앞서서 자료가 암호화됩니다. 일단 SSL 세션이 성립되면, 사용자 ID와 암호 교환을 포함하여 모든 Telnet 프로토콜이 암호화됩니다.

Telnet 서버를 사용할 때 고려해야 할 가장 중요한 요소는 사용자가 클라이언트 세션에서 사용하는 정보의 중요도입니다. 민감한 정보나 개인적인 정보인 경우에는 SSL을 사용하여 iSeries Telnet 서버를 설치하는 것이 유리합니다. Telnet 어플리케이션에 대해 디지털 인증을 구성하면, Telnet 서버가 SSL 클라이언트와 비SSL 클라이언트에서 모두 작동할 수 있습니다. 보안 정책에서 Telnet 세션을 항상 암호화하는 것을 요구할 경우에는 비SSL Telnet 세션은 모두 작동되지 않게 만들 수 있습니다. SSL Telnet 서버를 사용할 필요가 없을 때는 SSL 포트를 끌 수 있습니다. ADDTCPPORT 명령을 사용하여 포트를 작동 불가능하게 할 수 있습니다. 일단 포트를 끄고나면 서버가 클라이언트에 비SSL Telnet을 제공하므로 SSL Telnet 세션이 작동되지 않습니다.

Telnet에 대한 정보와 SSL을 사용하거나 사용하지 않는 Telnet에 대한 보안 관련 추가 정보는 다음 자원을 참조하십시오.

- Telnet Information Center 주제는 Telnet을 iSeries에서 사용할 때 필요한 정보를 제공합니다.
- Telnet 보안은 SSL과 Telnet을 함께 사용하여 Telnet 통신 세션을 보안하기 위한 정보를 제공합니다.
- TCP/IP 섹션의 iSeries 보안을 위한 추가 정보 및 툴  에 Telnet 보안에 대한 자세한 정보가 있습니다.

Client Access Express 보안을 위한 SSL

V4R4부터는 보안 소켓층(SSL)을 사용하도록 Client Access Express 서버를 구성하여 Client Access Express 통신 세션을 보안할 수 있습니다. 예를 들어, JKL Toy사는 회사가 성장해 감에 따라 많은 수의 지역 이동 판매 대리점들을 자사의 직원으로 추가했습니다. 이들 판매 대리점은 자신의 홈 오피스에서 장난감의 가용성과 제조 날짜의 상태에 관해 iSeries 생산 시스템의 정보에 액세스합니다. 그러나 자료의 민감성으로 인해 JKL Toy사에서는 판매 대리점들이 안전한 Client Access Express를 통해서만 정보에 액세스할 수 있도록 할 것입니다.

SSL 사용은 Client Access Express 세션에 대한 모든 통신의 암호화를 보장합니다. 즉, 자료가 로컬과 리모트 호스트 사이에서 전송되는 동안에는 자료를 읽을 수 없습니다.

SSL에서 Client Access Express를 사용하는 것에 대한 자세한 정보는 다음 자원을 참조하십시오.

- 보안 소켓층 관리

- Client Access Express 및 Operations Navigator 보안
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

개인 통신 보안을 위한 VPN(가상 사설망)

VPN(가상 사설망)을 사용하는 사람들이 점진적으로 증가하는 추세이며 VPN이 제공하는 보안 상의 이점으로 인해 JKL Toy사에서는 인터넷을 통해 전송되는 옵션에 대해 조사하고 있습니다. 이 회사는 최근에 자회사로 운영할 소규모의 장난감 제작 회사를 사들였습니다. 따라서 JKL에는 두 회사 사이에 정보를 전달해야 할 필요가 발생했습니다. 두 회사 모두 iSeries 시스템을 사용하므로 VPN 연결을 사용하여 두 네트워크 간의 통신에 보안을 제공할 수 있습니다. VPN을 작성하는 것은 기존의 전용 회선을 사용하는 것보다 비용면에서 훨씬 효율적입니다.

VPN 연결을 사용하여 지사, 모바일 직원, 공급자, 사업 파트너 등과의 연결을 제어하고 보안할 수 있습니다.

다음은 연결에 VPN을 사용할 때 혜택을 받을 수 있는 사용자들입니다.
- 리모트 사용자 및 모바일 사용자.
- 지사 또는 기타 오프사이트 위치에 대한 홈 오피스.
- 업무상 통신.

중요한 시스템에 대해 사용자 액세스를 제한하지 않으면 보안 위험이 발생합니다. 시스템에 액세스할 수 있는 사람들을 제한하지 않고서는 회사의 정보를 기밀로 유지하지 못할 수 있습니다. 시스템의 정보를 공유해야 할 사람들만 그 시스템에 액세스할 수 있도록 하는 계획이 필요합니다. VPN을 사용하여 인증 및 자료 보호(privacy) 등 중요한 보안 피처를 제공하는 동시에 네트워크 통신을 제어할 수 있습니다. 여러 개의 VPN 연결을 작성하여 연결할 때마다 시스템에 액세스할 수 있는 사람을 제어할 수 있습니다. 예를 들어, 회계 부서와 인사부의 경우 해당 부서가 소유하는 VPN을 통해 링크할 수 있습니다.

인터넷을 통해 사용자들이 시스템에 연결되도록 했을 경우 민감한 회사 자료가 공용 네트워크로 송신되어 공격에노출될 수 있습니다. 전송되는 자료를 보호하기 위한 하나의 옵션은 외부인으로부터 기밀을 보호하고 보안하기 위해 암호화 및 인증 방법을 사용하는 것입니다. VPN 연결은 특정 보안 요구, 즉 시스템 간 통신을 보안하기 위한 솔루션을 제공합니다. VPN 연결은 연결의 두 종료점 사이에서 흐르는 자료를 보호합니다. 그 외에도 패킷 규칙 보안을 사용하여 VPN 사이에 허용되는 IP 패킷을 규정할 수 있습니다.

VPN을 사용하여 보안 연결을 작성함으로써 제어를 받는 동시에 신뢰할 수 있는 종료점 사이의 통신을 보호할 수 있습니다. 그러나 VPN 상대에게 어느 정도의 액세스를 제공할 것인지가 여전히 문제입니다. VPN 연결은 자료가 공용 네트워크를 통해 흐르

는 동안 자료를 암호화할 수 있습니다. 그러나 구성 방법에 따라서 연결을 통해 통신하는 내부 네트워크에서 자료가 흐를 때 VPN 연결이 자료를 암호화하지 않을 수 있습니다. 결과적으로, 각 VPN 연결을 어떤 방식으로 설정할 것인지에 관해 세심하게 계획해야 합니다. VPN 상대에게는 본인이 의도한 내부 네트워크의 호스트 및 자원에 대한 액세스만 부여하십시오.

예를 들면, 사용자가 재고로 가지고 있는 부품에 관해 정보가 필요한 업체가 있을 수 있습니다. 따라서 인트라넷의 웹 페이지를 갱신하는 데 사용하는 데이터베이스에 이 정보를 보유합니다. 그 다음에는 이 업체가 VPN 연결을 통해 그 페이지에 직접 액세스하도록 할 것입니다. 그러나 데이터베이스 자체와 같이 다른 시스템 자원에 액세스하는 것은 원하지 않을 수 있습니다. 이 경우 두 종료점 사이의 통신을 포트 80으로 제한하여 VPN 연결을 구성할 수 있습니다. 포트 80은 HTTP 통신을 사용하는 디폴트 포트입니다. 결과적으로, 이 업체는 그 연결에서만 HTTP 요구와 응답을 송수신할 수 있습니다.

VPN 연결을 통해 흐르는 통신 유형을 사용자가 제한할 수 있으므로 연결에서 네트워크 레벨 보안 수단을 제공합니다. 그러나 VPN은 방화벽이 시스템 안과 밖에서 이루어지는 통신을 통제하기 위해 하는 것과 같은 방법으로 작동하지 않습니다. 뿐만 아니라 VPN 연결이 iSeries와 다른 시스템 간의 통신을 보한하기 위해 사용할 수 있는 유일한 수단은 아닙니다. 보안 요구에 따라서 SSL을 사용하는 것이 더 적절할 수도 있습니다.

VPN 연결을 통해 필요한 보안이 제공되는지의 여부는 보호하려는 대상에 따라 결정됩니다. 또한 그와 같은 보안을 제공할 때의 득실에 따라 달라집니다. 보안과 관련하여 이루어지는 다른 모든 결정과 마찬가지로 VPN 연결이 사용자의 보안 정책을 어떻게 지원하는지를 고려해야 합니다.

제 9 장 인터넷 보안 전문 용어

인터넷 보안 논의를 위한 기본 준비로서 인터넷 용어를 정의하는 것부터 시작하십시오. 인터넷 관련 용어를 이미 잘 알고 있다면, 이 섹션을 생략할 수 있습니다.

인증 인증은 리모트 클라이언트나 서버에 대해 실제로 권한이 있는 사람인지를 확인하는 처리입니다. 인증은 사용자가 현재 연결 중인 리모트 상대에 대한 신뢰성을 보장합니다.

크랙커 악의적인 의도를 가진 해커.

암호화 자료를 안전하게 유지시키는 기술. 암호화 처리는 관련되지 않은 사람들이 저장된 정보나 대화를 이해하지 못하게 하면서 다른 한편으로 정보를 저장하거나 다른 상대방과 대화할 수 있게 해줍니다. 암호화 처리는 이해가 가능한 텍스트를 이해가 불가능한 자료(ciphertext)로 변환시킵니다. 해독 처리는 이해할 수 없는 자료에서 이해할 수 있는 텍스트를 복원시킵니다. 두 프로세스 모두 수학적 공식이나 알고리즘 그리고 자료의 비밀 순서(키)가 관련되어 있습니다.

암호화 처리에는 다음과 같은 두 가지 유형이 있습니다.

- 공유/비밀 키**(대칭)** 암호 처리에서는 통신 당사자가 서로 하나의 키를 비밀로 공유합니다. 암호화 처리 및 해독에 같은 키를 사용합니다.
- 공용 키**(비대칭)** 암호화 처리에서는 암호화 처리 및 해독에 각각 서로 다른 키를 사용합니다. 따라서 당사자(party)가 공용 키와 개인 키의 두 키를 갖습니다. 두 키는 수학적으로 서로 관련이 있지만, 공용 키에서 개인 키를 파생시키는 것은 실질적으로 불가능합니다. 누군가의 공용 키로 암호화 처리한 메세지는 연관된 개인 키로만 해독할 수 있습니다. 또는 서버나 사용자가 개인 키를 사용하여 문서에 "서명"하고 공용 키를 사용하여 디지털 서명을 해독할 수 있습니다. 이와 같이 하여 문서의 소스를 검증합니다.

디지털 인증서

디지털 인증서는 신분증과 마찬가지로 인증서를 소유한 사람의 신분을 검증하는 디지털 문서입니다. 인증 기관(CA)이라고 하는 신뢰할 수 있는 제3자가 사용자와 서버에 대한 디지털 인증서를 발행합니다. CA에서 이루어지는 신임은 유효한 증명서로서 인증서에서의 신임의 기초가 됩니다. 따라서 다음과 같은 용도로 사용할 수 있습니다.

- 식별 - 사용자 식별
- 인증 - 사용자가 본인임을 확인
- 무결성 - 송신자의 디지털 "서명"을 검증하여 문서 내용의 수정 여부를 판별

- 비거부 - 사용자가 조치를 수행하지 않았다고 주장할 수 없음을 보증하는 것. 예를 들어, 자신이 신용 카드로 전자 구매를 승인한 경우 그 사실을 거부할 수 없게 만드는 것입니다.

디지털 서명

전자 문서에서 디지털 서명은 서면 문서에서의 개인 서명에 해당합니다. 디지털 서명은 문서가 원본임을 입증하는 것입니다. 인증서의 소유자가 그 인증서와 연관이 있는 개인 키를 사용하여 문서에 "서명"합니다. 그리고나면 문서 수신자가 이에 해당하는 공용 키를 사용하여 서명을 해독하여 원래 송신자가 맞는지 검증합니다.

DCM(디지털 인증 관리자)

디지털 인증 관리자는 OS/400을 로컬 인증 기관(CA)으로 허용합니다. DCM을 사용하여 서버나 사용자들이 사용할 디지털 인증을 작성할 수 있습니다. 다른 CA가 발행하는 디지털 인증을 가져오기 할 수 있습니다. 또한 OS/400 사용자 프로파일과 디지털 인증을 연관시킬 수도 있습니다. 그리고 통신을 보안하기 위해 DCM을 사용하여 보안 소켓층(SSL)을 사용하는 어플리케이션을 구성할 수 있습니다.

식별명 식별명은 인증 기관(CA)이 디지털 인증서를 발행하는 사람이나 서버의 이름입니다. 인증서의 소유권을 나타내기 위해 인증 시 이 이름이 제공됩니다. 인증서를 발행하는 CA의 정책에 따라서 식별명에 기타 권한 부여 정보가 포함되기도 합니다.

DNS(정의역명 서버)

인터넷에서 다른 DNS 서버와의 대화를 통해 인터넷 이름을 IP 주소로 변환하는 인터넷 호스트. 예를 들어, 많은 DNS 서버들이 다음을 인식할 수 있습니다.

```
vnet.ibm.com
```

그러나 다음과 같은 완전한 IP 주소를 아는 서버는 별로 없을 것입니다.

```
system1.vnet.ibm.com
```

인터넷에 접속할 때, 인터넷 클라이언트는 사용자가 통신하려는 호스트 시스템에 대한 IP 주소를 판별하기 위해 정의역명 서버를 사용합니다.

암호화 암호화는 올바른 암호해독 메소드가 없는 사람이 이해할 수 없는 형태로 자료를 변환합니다. 물론 권한이 없는 상대라고 하더라도 여전히 정보를 가로챌 수 있습니다. 그러나 올바른 암호해독 메소드가 없으면 정보를 이해할 수 없습니다.

엑스트라넷

기업 방화벽의 밖에 있는 여러 관련 조직의 업무용 사설 네트워크. 엑스트라넷 서비스는 표준 서버, 전자 우편 클라이언트 및 웹 브라우저를 포함한 기존 인

터넷 인프라구조를 사용합니다. 이것이 바로 엑스트라넷을 사용하는 것이 자사 소유의 네트워크를 만들어 유지보수하는 것보다 훨씬 경제적인 이유입니다. 엑스트라넷은 공통의 이익을 추구하는 무역 상대, 공급자 및 고객이 밀접한 사업적 관계와 강력한 통신 연대를 형성하기 위해 확장 인터넷을 사용할 수 있게 해줍니다.

방화벽 내부 네트워크 그리고 인터넷과 같은 외부 네트워크 사이의 논리적 장벽. 방화벽은 하나 이상의 하드웨어 및 소프트웨어로 구성됩니다. 방화벽은 보안된(또는 신뢰할 수 있는) 시스템과 보안되지 않은(또는 신뢰할 수 없는) 시스템 사이의 액세스와 정보 흐름을 제어합니다.

해커(hacker)

권한 없이 시스템에 침입을 시도하는 사람.

하이퍼텍스트 링크

정보의 한 부분(하이퍼텍스트 노드)과 다른 부분 간의 연결(하이퍼텍스트 링크)을 통해 온라인 정보를 제공하는 방법.

HTML(Hypertext markup language)

하이퍼텍스트 문서를 정의하는 데 사용되는 언어. HTML을 사용하여 문서의 외양(예: 강조표시 및 활자체) 및 기타 문서 또는 오브젝트에 대한 링크 방법을 표시합니다.

HTTP(하이퍼텍스트 전송 프로토콜)

하이퍼텍스트 문서에 액세스하기 위한 표준 방법.

인터넷 전세계적으로 상호 연결된『"네트워크들의 네트워크"』. 그리고 이 "네트워크들의 네트워크"에 연결된 컴퓨터가 서로 통신할 수 있게 하는 협조 어플리케이션의 모음. 인터넷은 찾아볼 수 있는 정보, 파일 전송, 리모트 로그온, 전자 우편, 뉴스 및 기타 서비스를 제공합니다. 인터넷을 때로는『넷(Net)』이라고도 합니다.

인터넷 클라이언트

요구를 발행하고 인터넷 서버 프로그램에서 결과를 수신하기 위해 인터넷을 사용하는 프로그램(또는 사용자). 클라이언트 프로그램마다 여러 가지 유형의 인터넷 서비스를 요구할 수 있습니다. 웹 브라우저는 클라이언트 프로그램의 한 유형입니다. FTP(파일 전송 프로토콜)는 또다른 유형입니다.

인터넷 호스트

인터넷이나 인트라넷에 연결되어 있는 컴퓨터. 인터넷 호스트가 둘 이상의 인터넷 서버 프로그램을 실행할 수도 있습니다. 예를 들어, 인터넷 호스트가 FTP 클라이언트 어플리케이션의 요구에 응답하기 위해 FTP 서버를 실행하는 경우가 있습니다. 또한 같은 호스트가 웹 브라우저를 사용하는 클라이언트의 요구에 응답하기 위해 HTTP 서버를 실행할 수 있습니다. 서버 프로그램은 일반적으로 호스트 시스템의 백그라운드에서(일괄처리로) 실행됩니다.

인터넷 키 교환(IKE)

IKE 프로토콜은 IPSec와 함께 사용되어 보안 협약의 자동 협상 뿐 아니라 암호 키의 자동 생성과 갱신을 지원합니다. 일반적으로, IKE는 가상 사설망의 일부로서 사용됩니다.

인터넷 이름

IP 주소에 대한 별명. IP 주소는 10.5.100.75와 같이 긴 숫자 양식으로서 기억하기가 어렵습니다. 이 IP 주소에 다음과 같은 인터넷 이름을 할당할 수 있습니다.

```
system1.vnet.ibm.com
```

인터넷 이름을 완전 규정 정의역명이라고도 합니다. 『저희 홈 페이지를 방문하십시오』라는 광고가 있을 때, "홈 페이지 주소"에 IP 주소가 아닌 인터넷 이름을 포함시키는 것을 볼 수 있는데, 이것은 인터넷 이름이 기억하기가 더 쉽기 때문입니다.

완전 규정 정의역명은 여러 부분으로 구성됩니다. 예를 들면, 다음과 같습니다.

```
system1.vnet.ibm.com
```

위에 나오는 예는 다음과 같은 부분들로 구성된 것입니다.

com: 모든 상용 네트워크. 정의역명 가운데 이 부분은 *인터넷* 기관(외부 조직)에서 할당합니다. 네트워크의 종류에 따라서 여러 가지 문자가 할당됩니다(상용의 경우 com, 교육 기관의 경우 edu).

ibm: 조직의 식별자. 정의역명의 이 부분도 인터넷 기관에서 할당하는 것으로서 고유합니다. 전세계에서 단 하나의 조직만 이 식별자를 사용할 수 있습니다.

```
ibm.com
```

vnet:

```
ibm.com
```

내의 시스템 그룹. 이 식별자는 내부적으로 지정된 것입니다. ibm.com의 관리자가 하나 이상의 그룹을 작성할 수 있습니다.

system1:

vnet.ibm.com 그룹 내의 인터넷 호스트 이름.

인터넷 서버

인터넷에서 해당 클라이언트 프로그램의 요구를 수용하고 인터넷에서 그 클라이언트에 응답하는 프로그램(또는 프로그램 세트). 인터넷 서버를 인터넷 클라이언트가 액세스하거나 방문할 수 있는 사이트로 생각할 수 있습니다. 다음과 같이, 서버 프로그램마다 서로 다른 서비스를 지원합니다.

- 찾아보기(『홈페이지』 그리고 다른 문서 및 오브젝트에 대한 링크).

- 파일 전송. 예를 들어, 클라이언트가 서버에서 클라이언트로 파일을 전송할 것을 요구할 수 있습니다. 파일은 소프트웨어 갱신사항, 제품 리스트 또는 문서일 수 있습니다.
- 정보를 요구하거나 제품을 주문하는 기능 등의 전자 상거래.

인터넷 서비스 제공자(ISP)

전화 회사에서 전세계 전화망과의 연결을 제공하는 것과 거의 같은 방법으로 인터넷과의 연결을 제공하는 조직.

인트라넷

웹 브라우저나 FTP와 같이 인터넷 툴을 사용하는 조직의 내부 네트워크.

IP 주소

인터넷 프로토콜(IP) 주소는 TCP/IP 네트워크에서 사용자를 알릴 수 있는 방법입니다. (인터넷은 아주 큰 TCP/IP 네트워크입니다.) 일반적으로 인터넷 서버에는 고유한 IP 주소가 할당되어 있습니다. 인터넷 클라이언트는 ISP가 할당하는 임시 IP 주소(하지만 고유한 IP 주소)를 사용할 수 있습니다.

IP 데이터그램

TCP/IP 네트워크를 통해 송신되는 정보 단위. IP 데이터그램(패킷이라고도 함)에는 자료 그리고 원점 및 목적지의 IP 주소와 같은 헤더 정보가 둘다 포함되어 있습니다.

IP 필터

IP 필터링은 방화벽에 대한 기본적인 보호 메카니즘을 제공합니다. IP 필터링을 통해 IP 세션 세부사항에 기초하여 어떤 통신이 통과하는지를 판별할 수 있습니다. 이것이 간단한 방법(예: 보안 서버 스캔)이나 아주 복잡한 방법(예: IP 주소 가장)을 사용하여 침투하는 외부인으로부터 보안 네트워크를 보호해줍니다. 필터링 피처를 다른 툴을 구축하기 위한 기초로서 생각하십시오. 필터링 피처는 크랙커로 판명된 사람의 액세스를 제외한 다른 모든 사람들에게 액세스를 부여하거나 거부하는 인프라구조를 제공합니다.

IPSec IP 층에서 패킷의 안전한 교환을 지원하는 프로토콜 세트. IPSec은 iSeries 및 기타 여러 시스템에서 VPN을 실행하는 데 사용하는 표준 세트입니다.

IP 가장

일반적으로 신뢰받는 시스템(IP 주소)인 것처럼 가장하여 시스템에 액세스하려는 시도. 일반적으로 침입자들은 사용자가 신뢰하는 IP 주소로 시스템을 설정합니다. 라우터 생산업체에서는 가장하여 침투하는 시도를 감지하고 거부하기 위해 시스템에 보안 장치를 내장하는 처리를 하고 있습니다.

네트워크 주소 변환(NAT)

프록시 및 SOCKS 서버를 위한 보다 투명한 대안을 제공합니다. 또한 호환되지 않는 주소지정 구조의 네트워크들을 연결할 수 있게 함으로써 네트워크 구성을 단순화합니다. NAT는 두 가지 주요 기능을 제공합니다. 내부 네트워크에

서 작동시킬 공용 웹 서버를 보호할 수 있습니다. NAT는 서버의 ″실제″ 주소를 일반인들이 사용할 수 있는 주소 뒤에 숨길 수 있게 함으로써 이 보호를 제공합니다. 또한 개인용 내부 IP 주소를 숨기는 반면에 내부 사용자들이 인터넷에 액세스할 수 있는 메카니즘을 제공합니다. NAT는 개인용 주소를 숨길 수 있게 함으로써 사용자가 내부 사용자들에게 인터넷 서비스에 액세스를 허용할 때 보호를 제공합니다.

비거부(Non-repudiation)

비거부는 트랜잭션이 발생했음, 메세지를 전송했음 또는 메세지를 수신했음을 증명하는 것입니다. 트랜잭션, 메세지, 문서에 대한 ″서명″을 위해 디지털 인증서와 공용 키 암호를 사용할 때 비거부가 지원됩니다.

패킷 이더넷 토큰 링이나 프레임 릴레이와 같은 회선 프로토콜에 관한 정보가 포함되어 있는 데이터그램.

프록시 프록시 서버는 보안 내부 네트워크의 클라이언트와 신뢰할 수 없는 네트워크의 서버 사이에서 요구를 재송신하고 응답하는 TCP/IP 어플리케이션입니다. 프록시 서버는 내부 네트워크 정보(예: 내부 IP 주소)를 숨기기 위해 TCP/IP 연결을 끊습니다. 사용자 네트워크 외부의 호스트는 프록시 서버를 통신 소스로서 인지합니다.

공용 키 인프라구조(PKI)

인터넷 트랜잭션에 포함되는 각 상대방의 유효성을 확인하고 인증하는 디지털 인증, 인증 기관 및 기타 등록 기관의 시스템.

보안 소켓층(SSL)

Netscape에서 작성한 SSL이 사실상 클라이언트와 서버 사이의 세션 암호화를 위한 업계 표준입니다. SSL은 서버와 클라이언트(사용자) 사이의 세션을 암호화하기 위해 대칭 키 암호화를 사용합니다. 클라이언트와 서버는 디지털 인증서를 교환하는 중에 이 세션 키를 협상합니다. 클라이언트와 서버 SSL 세션별로 서로 다른 키가 작성됩니다. 결과적으로, 권한이 없는 사용자가 세션 키를 가로채서 해독(거의 가능성이 없음)할 경우에도 현재, 미래 또는 과거의 SSL 세션에서 도청하기 위해 해당 세션 키를 사용할 수 없습니다.

탐지(Sniffing)

전자적 전송에서의 모니터링 또는 도청. 인터넷을 통해 송신되는 정보는 목적지에 도달하기 전에 많은 라우터를 통과할 수 있습니다. 라우터 생산업체, ISP, 오퍼레이팅 시스템 개발자들이 인터넷 백본에서 탐지 시도가 발생하지 않도록 하기 위해 계속해서 노력하고 있습니다. 그럼에도 불구하고 탐지 시도에 성공하는 사례가 점점 증가하는 추세입니다. 대부분 이와 같은 사고는 인터넷 백본 자체가 아니라 인터넷에 연결된 사설 LAN에서 발생합니다. 그러나 대부분의 TCP/IP 전송이 암호화 처리되어 있지 않으므로 탐지 발생 가능성에 유의해야 합니다.

SOCKS

SOCKS는 보안 게이트웨이를 통해 TCP/IP 통신을 전송하는 클라이언트/서버 구조입니다. SOCKS 서버는 프록시 서버가 수행하는 서비스의 많은 부분들을 처리합니다.

가장(Spoofing)

공격자가 사용자들이 자신을 믿고 비밀 정보를 송신하도록 설득하기 위해 신뢰할 수 있는 시스템으로 가장합니다.

TCP/IP

인터넷에서 사용되는 1차 통신 프로토콜. TCP/IP는 전송 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol)의 약자입니다. 내부 네트워크에서 TCP/IP를 사용할 수도 있습니다.

트로이 목마

트로이 목마는 시스템에 유용하면서도 해가 없는 기능을 수행하는 것처럼 나타나는 컴퓨터 프로그램입니다. 그러나 프로그램을 시작할 때 사용자에게 할당된 권한을 사용하는 숨겨진 기능이 있습니다. 예를 들어, 사용자 컴퓨터에서 내부 권한 부여 정보를 복사하고 그 정보를 트로이 목마의 작성자에게 다시 송신할 수 있습니다.

VPN(가상 사설망)

기업의 사설 인트라넷의 확장. 기본적으로 사설 "터널"을 통해서 보안된 사설 연결을 작성하여 인터넷과 같은 공용 네트워크에서 VPN을 사용할 수 있습니다. VPN은 시스템에 다른 사용자를 연결하는 인터넷을 통해서 안전하게 정보를 전달합니다. 다음과 같은 정보가 포함되어 있습니다.

- 리모트 사용자
- 지사
- 사업 상대 및 공급자

웹 브라우저

HTTP 클라이언트 어플리케이션. 웹 브라우저는 HTML을 해석하여 사용자를 위해 하이퍼텍스트 문서를 표시합니다. 따라서 사용자가 현재 문서의 영역을 클릭(또는 선택)하여 하이퍼링크 처리된 오브젝트에 액세스할 수 있습니다. 그 영역을 **핫 스팟**이라고도 합니다. 웹 익스플로러의 예로는 Internet Connection Web Explorer와 Netscape Navigator가 있습니다.

WWW(월드 와이드 웹)

문서 작성(HTML) 및 문서 액세스(HTTP)를 위해 같은 표준 형식을 사용하는 상호연결된 서버와 클라이언트의 망. 서버에서 서버로 그리고 문서에서 문서로 이루어진 연결 망을 비유적으로 **웹**이라고 합니다.

Printed in U.S.A