

# iQ

SMALL  
MEDIUM  
BUSINESS

Your Business Just Got Smarter  
SECOND QUARTER 2005

## A Better Way

DISCOVER THE POWER  
OF IP COMMUNICATIONS

PAGE 24

IAN SMITH, NEW YORK CITY  
ECONOMIC DEVELOPMENT  
CORPORATION

CISCO SYSTEMS



[CISCO.COM/GO/IQMAGAZINE](http://CISCO.COM/GO/IQMAGAZINE)

# 안전한

BY FRED SANDSMARK

# IP Communications

스마트한 기술과 적절한 방법으로  
음성 및 데이터에 보안 환경을  
제공합니다.

**비**용 절감과 뛰어난 생산성 향상을 통해 재빠르게 전화 기술이 진화 하고 있습니다. 기존의 회선 교환 음성 시스템은 VoIP 또는 IP Communications라고 불리는 인터넷 프로토콜(IP) 텔레포니 시스템으로 급격히 대체되고 있습니다. 이러한 기술 전환은 IP 기반 텔레포니의 상대적 보안에 대한 염려를 불러일으켰지만 많은 사람들은 이러한 염려가 근거 없는 것이라고 생각합니다. 적절한 보안을 사용하여 다른 네트워크 애플리케이션과 마찬가지로 음성 커뮤니케이션도 안전하게 보호할 수 있습니다. Burton Group의 수석 분석가인 Irwin Lazar는 “안전한 VoIP 환경을 배치할 수 있다는 확신을 사람들에게 심어줄 수 있는 제품이 속속 출시되고 있습니다. 뛰어난 기술과 스마트한 네트워크 관리를 결합하여 디지털/아날로그 세상에서 그 어떤 것보다도 안전한 음성 네트워크를 제공할 수 있습니다” 라고 말했습니다.

## IP Communications 측정

전화 시스템을 보호하기 위해서는 새로운 위협이 나타날 때마다 업데이트가 가능한 보안 기술이 필요합니다. 이런 이유 때문에 많은 전문가들은 IP Communications 시스템이 기존의 전화 시스템에 비해 더 안전하다고 생각합니다.



ILLUSTRATION BY YVETTA FEDOROVA

Lazar는 “[IP 기반 시스템]의 보안 옵션이 더 좋습니다” 라고 말했습니다. 그는 시스코 시스템즈를 비롯한 IP 텔레포니 제조업체가 보안 기술을 지속적으로 개선하고 있다고 강조했습니다. 예를 들어, 침입자가 전화선을 도청하거나 전화 스위치 클로짓에 실제로 들어가더라도, 암호화를 사용하여 적절하게 보호된 IP Communications 시스템에서는 이 침입자가 통화를 엿들을 수 없습니다.

기존의 전화 시스템과 달리 IP Communications 시스템은 표준 기반의 IP 네트워크에 구축됩니다. 엔지니어는 내외부 위협으로부터 네트워크를 보호하기 위해 오랫동안 노력했습니다. 그 결과, 이 시스템은 기존의 전화 시스템에 비해 보안 위협을 더 효과적으로 줄일 수 있습니다.

예를 들어, 방화벽은 네트워크의 경계를 보호합니다. 방화벽은 네트워크상의 이상 동작이나 트래픽을 감지하고 시스템에 대한 불법 액세스를 차단합니다. IP Communications 환경에서 방화벽은 엄청난 양의 음성 트래픽을 관리해야 하므로 방화벽이 적절하게 관리되고 구성되어야 합니다. 컴퓨터 바이러스와 웹의 위협이 심각하기 때문에 IP 시스템은 이러한 유형의 위협도 지속적으로 모니터링합니다.

또한, IP Communications 시스템을 관리하는 사람은 대체로 보안 중심의 시각을 가지고 있습니다. Sage Research의 연구 책임자인 Chris Neal은 “[IP Communications]를 운영하는 사람은 대개 음성 쪽보다는 IT/데이터 쪽 출신입니다” 라고 말했습니다. “이 분야 사람은 기존 PBX를 관리해 왔던 전문가에 비해 한 곳만을 집중하는 편집증적인 증상이 있습니다.”

#### 통합 보안

앞서가는 IP Communications 시스템에서는 통화 설정 시와 통화 중에 통화의 프라이버시를 보장하기 위해 암호화 기술을 사용합니다. Lazar는 “VoIP 장비의 대부분의 주요 벤더는 완벽한 통화 암호화를 위한 성능과 통화 설정을 위한 신호 방식을 현재 보유하고 있거나 앞으로 보유할 것입니다. 시스코는 현재 통화 암호화를 지원합니다” 라고 말했습니다. 일부 IP Communications 사용자는 암호화 기능을 사용하기를 원치 않지만 특히 관리, R&D, 금융 등의 분야에서는 이 기능이 중요합니다.

IP Communications 기술의 사용을 좌지우지하는 정책을 구현하는 것은 보안 문제를 해결하는 데도 도움이 됩니다. 예를 들어, 시스템에 대한 액세스는 기업 내 개별 역할에 따라 달라져야

합니다. 경영 보좌관이 CIO와 동일한 액세스 권한을 가져서는 안 됩니다. 음성 및 데이터는 동일한 네트워크를 공유하므로 더욱 광범위한 네트워크 보안 전략에 IP Communications를 통합해야 합니다. 많은 기업은 중앙에서 관리되는 통합 보안을 구현하면 전체적인 보안 요구사항을 떨어뜨리지 않고도 시간과 비용을 줄일 수 있음을 알았습니다.

### TALK TO A CISCO EXPERT

IP Communications의 보안에 대한 자세한 내용은  
1-800-745-8308, 내선 번호 4602로 문의하십시오.

보안의 대부분을 차지하는 것은 네트워크 및 통화 제어 시스템에 기본적으로 내재된 보안입니다. 네트워크가 적절하게 설계되고 관리되면 암호화되거나 되지 않은 음성 트래픽의 도청 가능성이 상당히 줄어듭니다. 바로 이 때문에 IP Communications를 사용하는 실제 기업에서는 보안이 최우선 문제가 되지 않습니다. IP Communications를 보유한 수백 곳의 기업을 인터뷰했던 Neal은 “IP 텔레포니 시스템에서 심각한 보안 문제가 발생했다는 얘기는 들어본 적이 없습니다” 라고 말했습니다.

Fred Sandmark는 샌프란시스코 만 지역에 거주하며 iQ Magazine에 정기적으로 글을 기고하고 있습니다.

#### 다음 단계

타 산업에 종사하는 세 SMB에서 IP Communications의 비즈니스 이점을 어떻게 활용했는지 읽어보십시오 (24페이지의 “The Future Calls” 참조). 시스코 통합 서비스 라우터에 대한 자세한 내용은 [cisco.com/go/iq-isr](http://cisco.com/go/iq-isr)을 참조하십시오.

#### FROM CISCO

### 음성 커뮤니케이션을 보호하는 시스코

IP Communications 환경에서는 전자 메일, 음성 커뮤니케이션, 서버 및 개별 컴퓨터를 보호하기 위해 중앙 관리 통합 보안을 사용하는 것이 개별 제품을 사용하는 것보다 기술적으로나 경제적으로 더 효율적입니다. 이런 이유 때문에 SMB 용으로 설계된 일부 시스코 통합 서비스 라우터는 IP Communications 기능뿐만 아니라 광범위한 보안 기능을 지원합니다. 이 라우터는 업계에서 가장 폭넓고 광범위 하며 동급 최강의 라우팅 기능과 통합된 보안을 제공합니다. 시스코의 통합 보안 솔루션은 원격 작업자 연결을 위한 VPN

(Virtual Private Networks) 기술, 네트워크에 대한 불법 액세스를 차단하는 방화벽 그리고 네트워크 공격을 자동으로 감지하고 차단하는 시스코 IPS(Intrusion Prevention System)을 포함합니다. 다른 보안 제품과 통합할 수도 있습니다.

시스코는 IP Communications에 적합한 두 계층의 통합 서비스 라우터를 보유하고 있습니다. 2800 시리즈는 최대 96개, 3800 시리즈는 최대 240개의 IP 폰을 처리합니다. 광범위한 보안 이외에도 유선속도로 작동하므로 케이블 연결만큼

빠른 속도로 정보를 처리할 수 있습니다. 보안 관련 지연이 발생하지 않는 뛰어난 네트워크 성능을 제공합니다.

또한, 통합 서비스 라우터는 가장 까다로운 엔터프라이즈 환경을 충족시키기 위해 확장이 가능하므로 SMB 투자도 보호할 수 있습니다. 이 라우터는 미래의 새로운 서비스를 수용하도록 설계되었으며 모든 조직에 안전한 음성 성능을 제공하는 기반입니다.