

## Data Sheet

### Cisco IOS Firewall

안전한 업무 진행을 위해 네트워크 보안이 갈수록 중요해짐에 따라 기업들은 보안을 네트워크 설계 및 인프라 자체에 통합해야 합니다. 보안 정책이 네트워크 자체에 포함될 경우 가장 효과적으로 실행될 수 있습니다. Cisco IOS® Firewall 은 Cisco IOS Software 를 위한 보안 전용 옵션입니다. 이 옵션은 모든 네트워크 외곽을 위한 강력한 방화벽 기능과 침입 탐지 기능을 통합시켜줍니다. 또한, 상태 보존형 애플리케이션 기반 필터링, 동적 사용자 별 인증 및 권한 부여, URL 필터링 등의 최첨단 보안 기능을 제공함으로써 기존 Cisco IOS 보안 솔루션(예: 인증, 암호화, 장애 복구)에 깊이와 유연성을 더해줍니다. Cisco IOS IPSec 이나 L2TP 터널링 및 서비스 품질(QoS)과 같은 Cisco IOS 기술과 결합할 경우 Cisco IOS Firewall 은 완전한 통합 가상 사설망(VPN) 솔루션을 제공합니다.

### 라우터 기반 방화벽 기능

Cisco IOS Firewall 은 다양한 Cisco IOS Software 버전에서 제공됩니다. 조직 내(인트라넷)에서의 연결과 파트너 네트워크(엑스트라넷)는 물론, 원격 또는 지사 사무실의 인터넷 연결을 보호하기 위한 첨단 보안 및 정책 실행 기능을 제공합니다.

Cisco IOS Firewall 은 멀티프로토콜 라우팅을 보안 정책 실행 기능과 통합하고 관리자들이 시스코 라우터를 방화벽으로 설정할 수 있는 최고의 제품입니다. 또한, 고객들은 대역폭, LAN/WAN 밀도, 멀티서비스 요건을 기반으로 라우터 플랫폼을 선택할 수 있는 고급 보안 기능의 혜택도 선사합니다.

여러 가지 보안 환경에 적합한 시스코 라우터를 선택하려면 다음 가이드라인을 참조하십시오:

- 소규모/재택 근무 사무실: Cisco 800, UBR900 및 1700 Series Routers
- 지사 및 엑스트라넷 환경: Cisco 2600, 3600 및 3700 Series Routers
- VPN 및 WAN 애그리게이션 지점이나 기타 처리량이 높은 환경: Cisco 7100, 7200, 7400, 7500, RSM Series Routers; Cat 5k 및 Cat6k 스위치

### 주요 혜택

Cisco IOS Firewall 은 Cisco IOS Software 와 자연스럽게 상호 운용되어 뛰어난 가치 및 혜택을 제공합니다:

- **유연성** - Cisco IOS Firewall 을 시스코 라우터에 설치할 경우, 멀티프로토콜 라우팅, 경계 보안, 침입 탐지, VPN 기능, 사용자 별 인증 및 권한 부여 기능을 실행하는 확장 가능한 올인원 솔루션이 됩니다.
- **투자 보호** - 방화벽 기능을 멀티프로토콜 라우터에 통합시킴으로써 기존 라우터 투자를 활용, 새로운 플랫폼 도입에 따르는 비용이나 적응 시간이 필요 없게 됩니다..
- **VPN 지원** - Cisco IOS Firewall 을 Cisco IOS 암호화 및 QoS VPN 기능과 함께 설치하면 저렴하고 안전하게 공공 네트워크를 통해 데이터를 전송할 수 있게 됩니다. 또한, 업무에 중요한 애플리케이션의 트래픽이 우선 순위를 갖도록 합니다.

- **확장성 있는 설치** - Cisco IOS Firewall 은 폭넓은 라우터 플랫폼에서 제공됩니다. 모든 네트워크의 대역폭 및 성능 요건을 만족시킬 수 있도록 확장할 수 있습니다.
- **용이한 프로비저닝** - Cisco IE2100 과 Cisco IOS XML 애플리케이션을 혼합하면 네트워크 관리자가 사전 설정을 거의 하지 않고도 모든 시스코 라우터를 추가할 수 있습니다. 라우터는 인터넷과 연결된 후 방화벽을 위한 가장 최신 Cisco IOS Software 버전의 라우터 설정 및 보안 정책 설정을 가져옵니다.

Cisco IOS Firewall 은 대부분의 시스코 라우터 플랫폼에서 지원되므로 멀티서비스 통합(데이터/음성/비디오/다이얼), 다이얼업 연결을 위한 고급 보안 등을 포함하는 중요한 혜택을 선사합니다. Cisco 7100, 7200 및 7400 Series Routers 에서는 대기업을 위한 인터넷 게이트웨이에서 통합된 라우팅과 보안, 서비스 공급업체 CPE(customer premise equipment) 등의 추가적인 혜택을 제공합니다.

## Cisco IOS Firewall 의 주요 기능

**Stateful IOS Firewall 검사 엔진** - 내부 사용자들에게 경계(예: 사설 기업 네트워크와 인터넷 간의 경계) 상의 모든 트래픽에 대한 안전한 애플리케이션 별 기반 액세스 제어를 제공합니다. 이는 CBAC(Context-Based Access Control)로도 알려져 있습니다.

**침입 탐지** - 가장 일반적인 공격 및 정보 수집을 위한 침입 탐지 서명을 이용, 네트워크 오용에 대한 실시간 모니터링, 차단 및 대응을 제공하는 인라인 딥(deep) 패킷 검사 서비스입니다. 현재 102 개의 서명을 지원합니다.

**방화벽 음성 통과** - 콜 흐름과 관련된 열린 채널에 대한 애플리케이션 수준의 프로토콜 인텔리전스를 통해 제공됩니다. 현재 지원되는 음성 프로토콜은 H.323v2 와 SIP (Q1CY03)입니다.

**ICMP 점검** - 다른 ICMP 트래픽은 거부하면서 방화벽 내에서 발생한 ICMP 패킷(예: 핑과 Traceroute)에 대한 응답을 허용합니다. 2003 년 1/4 분기에 제공됩니다.

**인증 프록시** - LAN 기반 http 및 다이얼 인 통신을 위한 동적인 사용자 별 인증 및 허가를 가능케 하며 업계 표준을 통해 사용자를 인증합니다. Http 를 위한 SSL 보안 사용자 ID 와 패스워드(HTTPS) 지원은 더욱 확실한 보안성을 제공합니다. TACACS+와 RADIUS 인증 프로토콜은 네트워크 관리자들이 개별적인 사용자 별 보안 정책을 설정할 수 있도록 합니다. HTTPS(SSL 보안 http)는 2003 년 1/4 분기에 지원됩니다.

**목적지 URL 정책 관리** - 이전 요청에 대한 로컬 캐싱, 사전에 결정된 정적 URL 허가 와 거부 테이블, Websense Inc. 및 N2H2 Inc.에서 제공하는 외부 서버 데이터베이스 이용을 지원하는 다양한 메커니즘입니다. 이는 URL 필터링으로 더 잘 알려져 있습니다. 2003 년 1/4 분기부터 모든 플랫폼에서 제공됩니다.

**사용자 별 방화벽** - 인증 후 AAA 서버 프로필 스토리지를 이용, 고유의 방화벽, ACL 및 기타 설정을 사용자 별로 다운로드하여 서비스 공급업체들이 광대역 시장에서 관리 방화벽 솔루션을 제공할 수 있도록 합니다.

**Cisco IOS 라우터 및 방화벽 프로비저닝** - 라우터의 제로(0) 터치 프로비저닝, 버저닝, 방화벽 규칙과 같은 보안 정책을 제공합니다.

**서비스 거부 탐지 및 방지**- 일반적인 공격으로부터 라우터 자원을 방어 및 보호하고, 패킷 헤더를 확인하며, 의심되는 패킷을 드롭합니다.

**동적 포트 매핑** - 비표준 포트 상에서 방화벽 지원 애플리케이션을 허용합니다.

**자바 애플릿 블로킹** - 확인되지 않은 악의적인 자바 애플릿에 대한 방어를 제공합니다.

#### **VPNs, IPSec 암호화 및 QoS 지원 -**

Cisco IOS Software 암호화, 터널링 및 QoS 기능과 함께 작동하여 VPN 을 보호합니다.

강력한 경계 보안, 고급 대역폭 관리, 침입 탐지 및 서비스 레벨 확인을 통합하는 동시에 라우터 상에서 확장 가능한 암호 터널을 제공합니다.

상호운용성을 위한 표준을 기반으로 하고 있습니다.

**실시간 경보** - 서비스 거부 공격이나 기타 설정된 조건에 대한 로그 경보를 제공합니다. 애플리케이션 별, 기능 별로 설정할 수 있습니다.

**감사 트레일** - 세밀한 보고를 위해 트랜잭션에 대한 세부 설명과 함께 타임 스탬프, 소스 호스트, 목적지 호스트, 포트, 지속 시간 및 전송된 전체 바이트 수를 기록합니다. 애플리케이션 별, 기능 별로 설정할 수 있습니다.

**Cisco IOS Software 와의 통합** - Cisco IOS Software 기능과 상호 운용되어 네트워크 내에 보안 정책 실행을 통합합니다.

#### **기본 및 고급 트래픽 필터링 -**

표준 및 확장된 액세스 제어 목록(ACL) - 액세스 제어를 특정 네트워크 세그먼트에 적용하며 어떤 트래픽이 네트워크 세그먼트를 통과할지 정의합니다.

락(Lock)과 키(Key) - 동적인 ACL 은 사용자 인증(사용자 이름/암호)에 따라 방화벽을 거치는 임시 액세스를 제공합니다.

**정책 기반 멀티 인터페이스 지원** - 보안 정책에 따라 IP 주소와 인터페이스 별로 사용자 액세스를 제어할 수 있는 기능을 제공합니다.

**NAT(Network Address Translation)**- 향상된 보안을 위해 내부 네트워크를 외부로부터 숨깁니다.

**시간 기반 액세스 목록** - 시간 및 요일에 따라 보안 정책을 정의합니다.

**피어(peer) 라우터 인증** - 라우터가 신뢰된 소스로부터 신뢰할 수 있는 라우팅 정보를 받도록 합니다.