Anti-DDoS에서 VoIP 보안까지

나우콤
나우콤
나우콤

경제위기와 더불어 기업과 개인이 다양한 보안위협에 노출됨에 따라 지난 2008년은 1.25 인터넷 대란 이후 정보보호가 다시 한번 사회적 이슈로 떠오른 해였다. 협박성 대량 트래픽 공격(DDoS : 분산서비스거부공격)에 의한 웹 서비스의 불안정, 급속도로 이용자가 늘고 있는 인터넷전화(VoIP)의 보안위협까지. 기업과 일반 IT 제품 및 서비스 이용자들은 직간접적으로 보안이슈에 노출되고 있다.

조현정 | 나우콤 과장_ajanee@nowcom.co.kr

DDoS 공격은 지난해부터 웹하드, 게임아이템 거래사이트 등을 대상으로 금전을 요구하는 악의적 목적으로 이용되고 있으며, 증권사 웹 사이트, 게임아이템거래사이트, 공공기관 등 그 대상과 피해가 확대되고 있는 실정이다. 또 인터넷을 이용해 음성을 송수신하는 VoIP는 일반 가정 내 전화에서 발생할 수 있는 도·감청 등의 위협 뿐 아니라 인터넷상에서 발생할 수 있는 각종 해킹 위협에 노출되어 있는 것으로 알려져 있다. 대량 스팸, 특정 단말기나 교환시스템에 대한 플루딩(Flooding) 공격, SIP(Session Initiation Protocol) 취약점을 이용한 서비스거부공격(DoS), 인증 취약성을 이용한 과금 회피 등이 최근 제기되는 보안 이슈들이다.

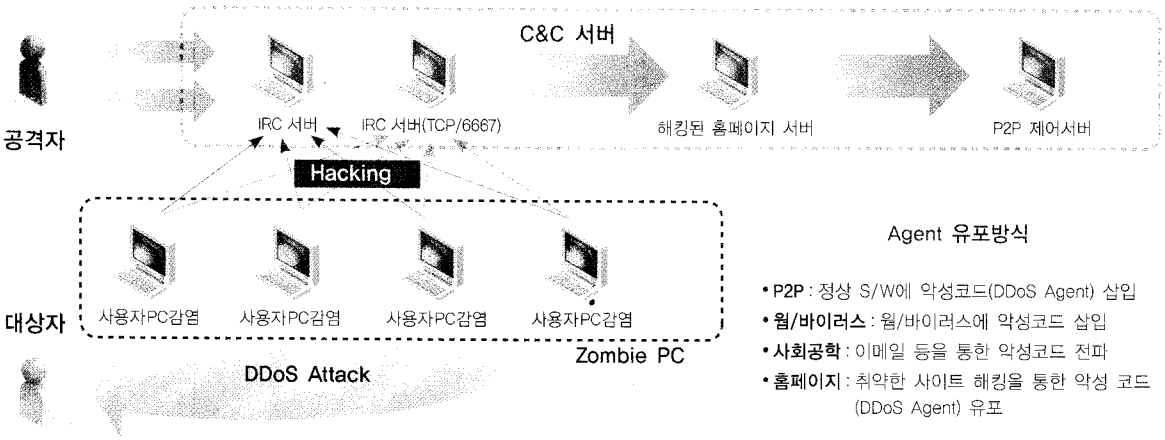
물론 새로운 '창'을 막기 위한 '방패' 역시 더욱 더 발전하기 마련이다. 스나이퍼 시리즈로 이미 잘 알려진 나우콤은 지난해 국내 보안업체로는 드물게 안티 DDoS 장비 '스나이퍼 DDX'를 개발하는 한편, VoIP 전용 IPS '스나이퍼IPS-V를 개발, 새로운 위협에 대응하고 있다. 10기가비트 트래픽 처리기술을 개발해 안티 DDoS와 IPS 제품에 적용, 10G 고성능 모델까지 출시하는데 성공했다. 최근 DDoS 공격 등 대용량 트래픽 공격 성행과 대용량 인터넷 인프라의 확산에 따라 인터넷서비스사업자(ISP), 전자상거래 및 오픈마켓, 학내 망 등을 중심으로 10G 보안장비는 수요가 늘고 있으며, 특히 공공기관의 망 분리사업의 일환으로 네트워크 인프라가 10G로 전환되면서 공공기관의 10G 보안제품 수요도 상승세를 타고 있다.

안티 DDoS : 분산서비스거부공격 차단시스템

DDoS 공격은 높은 수준의 해킹 능력이나 시스템 이해도가 필요한 공격이 아니다. 단지, TCP/IP 프로토콜 스택의 연결 성립 메커니즘의 구조적 취약점을 이용한 공격이다. 이로 인해 정상적인 대용량 트래픽과 DDoS 공격에 이용된 비정상적인 해킹 트래픽을 구분하는 것은 매우 어려우며, 모든 시스템과 네트워크가 DDoS 공격으로부터 완전히 자유로울 수는 없다. 때문에 구분이 모호한 트래픽에 관한 명확한 분석 알고리즘과 네트워크 및 시스템의 가용성을 보장하기 위한 여러 가지 보완책이 필요하며, 공격 발생 시 피해를 최소화하기 위한 최선의 대응책을 마련하는 것이 바람직하다.

한편 DDoS 공격을 막는 장비들도 잇따라 출시되고 있는데, 여기에는 전제조건이 필요하다. DDoS 공격이 대량의 트래픽을 이용하는 만큼 차단장비의 성능이 보장되어야 한다는 것이다. 특히 일부 DDoS 공격 차단기능을 제공하는 제품의 경우, 보안제품 본연의 기능을 수행하면서 부가적으로 DDoS를 차단한다는 점에서 DDoS 발생 시 장비 자체의 다운이나 본연의 기능 수행이 불가능할 수 있어 위험할 수 있다.

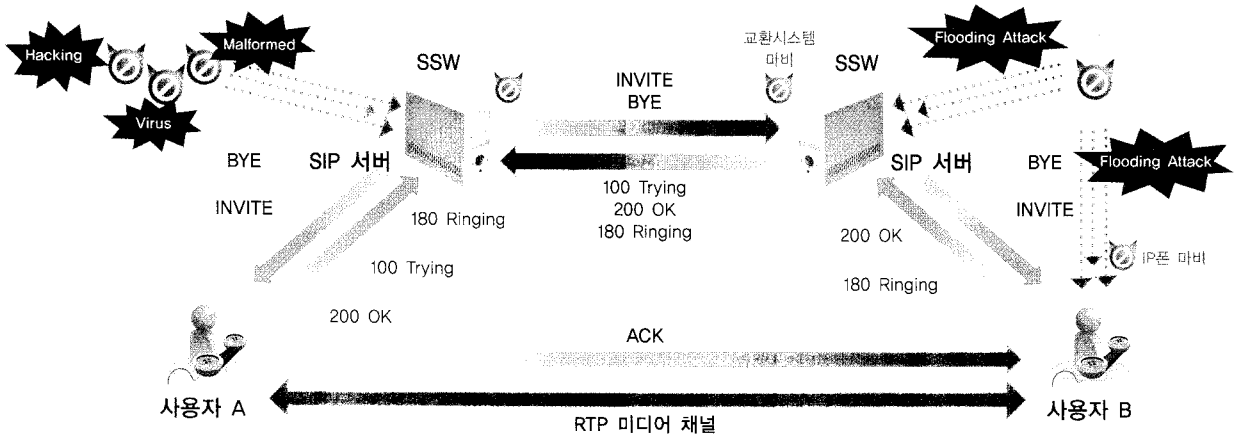
나우콤의 '스나이퍼DDX'는 대표적인 DDoS 차단 전용장비로, 1.5G 성능에서부터 10G까지 다양한 규격의 모델로 구성되어 있다. 지난해 11월 CC평가계약을 체결해 오는 4~5월경 인증이 완료될 예정으로, 향후 공공 및 금융권 수요에 적극적으로 대응할 수 있을 전망이다.



▲ DDoS 공격 형태

VoIP 전용 IPS : 인터넷전화망 전용 침입방지시스템

VoIP는 음성 프로토콜을 이용한 인터넷전화로 지난해 VoIP 번호이동제 시행 이후 이용자가 급속도로 늘고 있다. 하지만 전문가들이 VoIP의 보안문제를 잇따라 지적함에 따라 이를 위한 보안제품의 필요성이 대두됐다. VoIP는 인터넷을 이용해 음성을 송수신하기 때문에 인터넷상에서 발생할 수 있는 각종 해킹 위협까지 그대로 적용될 수 있어 시스템 도입 시 보안은 가장 중요한 선결과제라고 할 수 있다.



▲ VoIP 이용을 위협을 하는 공격형태

2007년까지만 해도 주요 ISP의 VoIP 망 구성에 따라 기존 IPS에 VoIP 트래픽 분석기능을 추가해 커스터마이징 형태로 공급했으나, 보안의 중요성이 증가됨에 따라 지난 2008년 하반기부터 VoIP 전용 보안제품이 개발되고 있다. 물론 VoIP 전용 보안제품은 VoIP 트래픽 특성에 최적화된 보안기능을 제공하는 것을 의미한다. 2년의 개발기간을 거쳐 출시된 나우콤의 VoIP 전용 IPS는 음성뿐만 아니라, 일반 프로토콜까지 분석 및 통제가 가능하다는 장점을 갖고 있다.

이처럼 최신 보안위협 및 시장 이슈에 부합하는 첨단 보안기술과 제품 개발에 적극적인 나우콤은 올해도 지속적 제품관리와 품질개선으로 경쟁력을 높이고, 꾸준한 연구개발(R&D) 투자로 새로운 보안위협에 대응하는 '방패'를 지속적으로 개발할 계획이다. S