정규표현식 전수조사 방식의 유일한 보안 솔루션

SoliGate™ RxIPS

고객의 네트워크 안정성을 보장하는
정규표현식 전수조사 기반의 **침입방지시스템**

INFNIS

㈜인프니스네트웍스

지금까지 국내외의 침입방지시스템(IPS/IDS)의 공격 탐지 방식으로 오픈 소스인 스노트(Snort) 스타일이 가장 많이 쓰이고 있습니다. 그런데 문제는 이 스노트 방식이 전혀 보안에 안전하지 않다는 점입니다. 스노트 방식은 선별된 일부 네트워크 데이터 패킷에 대해서만 위험을 살펴보는 **표본조사(sampling inspection)**입니다. 모든 데이터에 대해서 공격성을 판정하는 **전수조사(total inspection)**가 당연한데도 지금까지는 기술적 한계로 전수조사를 하지 못하였습니다. Soligate RxIPS는 전세계 최초이자 유일한 **정규표현식 전수조사** 기반의 침입방지시스템입니다.

스노트 방식의 표본조사는 전수조사가 기술적으로 어려운 제약 조건에서 궁여지책으로 사용되어 왔습니다. 최근에는 공격의 유형이 점점 복잡해져서 상세 조사를 위한 표본 선정이 쉽지 않고, 이 때문에 표본조사를 통해 성능 저하를 막으려는 시도는 불가능해졌습니다.

표본조사 방식에서는 데이터의 공격 여부를 살펴보기 전에 조사 대상인 표본 선정의 불필요한 절차가 수반되는데, 이로 인해 수천 개 이상되는 탐지룰을 체계적으로 관리할 수가 없습니다.

빈번한 성능 저하
유사, 중복 탐지룰로 관리 어려움
DoS 공격의 대상, APT 공격에 취약
비효율적 메모리 사용

〈스노트 방식 표본조사의 취약점〉

가장 큰 문제는 보안상의 허점입니다. 보안 제품은 다른 것은 다 양보해도 보안성만은 지켜내야 합니다. 그런데, 표본조사 방식은 공격자가 임의로 선정되는 표본의 수를 많게 하여 침입방지시스템 자체가 느려지도록 만드는 DoS 공격에 아주 취약합니다. 좀비 PC 몇 대만으로도 스노트 방식의 침입방지시스템을 무력화시킬 수 있습니다. 표본 선정 과정에서는 고정된 단순 문자열을 포함하기만 하면 표본으로 판정하기 때문에, 공격자가 정상 데이터에 이 문자열을 포함시킨다면 선정되는 표본의 수가 손쉽게 늘게 됩니다. 침입방지시스템 자체가 DoS 공격의 대상이 되어 무력화되는 것입니다.

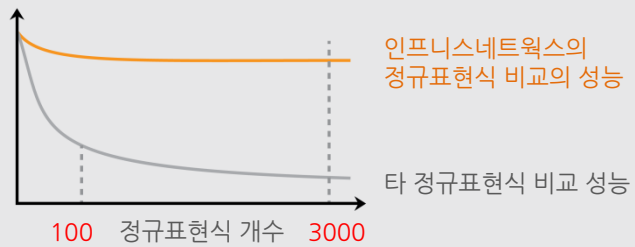
게다가 표본 선정 과정에서는 사용되는 문자열(키워드)이 해커들에게 대부분 노출되어 있어서 APT(지능형 지속 위협) 타입의 해커 공격에 매우 취약합니다. 스노트의 탐지룰은 공개되어 있고, 스노트 방식을 취하는 대부분의 침입방지시스템들이 사용하는 표본 선정용 문자열도 스노트와 유사하기 때문에, 특정 사이트를 침입하려는 숙련된 해커라면 해당 시스템의 문자열을 시간을 들여서라도 알아낼 수 있습니다. 해커가 공격 데이터가 이 문자열을 포함하지 않도록만 하면 스노트 방식의 시스템은 안전한 데이터로 판정하기 때문에 공격에 손쉽게 성공할 수 있는 것입니다.

더 이상, 스노트 스타일의 표본조사 제품은 네트워크를 보호하지 못합니다. 모든 데이터를 일일이 다 조사하는 전수조사만이 네트워크를 제대로 보호할 수 있습니다. 인프니스네트웍스의 Soligate RxIPS는 유일한 전수조사 방식의 보안 솔루션입니다.

Soligate RxIPS는 정규표현식(PCRE) 비교로 모든 데이터를 전수조사합니다.

스노트와 같은 표본조사 방식이 지금까지 널리 사용된 이유는 그동안 정규표현식 비교 성능이 낮았기 때문입니다. 스노트는 선정된 표본에 대해서만 선별적으로 PCRE(펄 호환 정규표현식, Perl Compatible Regular Expressions) 비교를 합니다. PCRE는 가장 널리 사용되는 정규표현식의 한 버전입니다.

일부 업체들은 스노트 방식의 표본조사이면서 마치 PCRE 비교로 보안성이 강화된 것처럼 과장되게 홍보하고 있습니다. 아무리 정규표현식 비교를 하더라도 모든 패킷에 대해서 하지 않으면 아무 소용이 없습니다. 인프니스네트웍스의 Soligate RxIPS는 PCRE 비교, 즉 정규표현식 비교를 모든 패킷에 수행하는데 이는 독자적이고 혁신적인 정규표현식 비교 기술을 다년간 연구하고 상업적 응용에 성공했기에 가능하게 되었습니다.



〈㈜인프니스네트웍스의 혁신적인 정규표현식 비교 성능〉

지금까지 기술은 정규표현식 또는 PCRE의 패턴의 수가 100개가 넘어가면 비교 성능이 급격히 하락하여 적용이 거의 불가능하였습니다. 그런데, 인프니스네트웍스의 혁신적인 정규표현식 비교 기술은 패턴의 개수가 3000개가 넘어도 성능 저하가 거의 없습니다. 학계와 업계가 깜짝 놀라는 이와 같은 높은 성능은 인프니스네트웍스가 지난 수년간 학계의 연구자와 함께 공동으로 이루어낸 자랑스러운 성과입니다.

높은 성능의 정규표현식 비교 성능을 바탕으로, 오직 인프니스네트웍스의 RxIPS만이 유일하게 정규표현식 전수조사를 수행합니다. 정규표현식으로는 가장 널리 사용되는 PCRE 문법을 지원합니다. 정규표현식 전수조사는 스노트의 표본조사가 갖고 있는 많은 취약점을 해결하는 유일한 대안입니다.

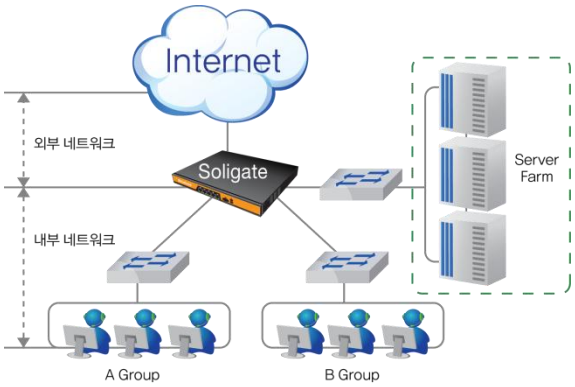
이제는 정규표현식 전수조사 방식의 침입방지시스템(IPS/IDS)을 도입해야만 네트워크를 보호할 수 있습니다. 인프니스네트웍스의 Soligate RxIPS가 유일한 답입니다.

	스노트 방식 ***표본조사***	**인프니스네트웍스 Soligate RxIPS** ***전수조사***
성능	표본 선정이 많아져서 **급격한 성능 저하**	**성능 저하 없음**
탐지룰 작성	표본 선정용 문자열 추출의 **비과학적인 수작업**	**공격 분석에 따른 정규표현식 작성의 과학적인 과정**
탐지룰 관리	표본 선정용 문자열로 인한 **중복, 유사 탐지룰 증가** (비효율적 룰 관리)	**공격 유형별 탐지룰 관리** (효율적 탐지룰 관리)
보안성	**DoS 공격 대상** **APT 공격 취약**	**보안성 강화**
메모리 사용 측면	문자열 비교, 정규표현식 비교의 이중 사용으로 인한 **비효율적 메모리 사용**	전수조사 방식의 **효율적 메모리 사용**

Soligate RxIPS는 정규표현식(PCRE문법) 기반으로 사용자 정의 탐지룰 작성을 지원합니다.
일반적인 침입방지시스템(IPS/IDS)이 지원하는 탐지룰을 포함하며, 약 20개 카테고리에 3,000개 이상의 탐지룰을 운영할 수 있습니다. 또한, 사용자 정의 룰을 작성 기능을 이용하여 관리자가 필요로 하는 탐지룰을 직접 입력할 수 있으며 정규표현식(PCRE문법)으로 바로 입력할 수 있습니다.

정규표현식 전수조사 탐지룰	정규표현식(PCRE문법) 탐지룰로 변종, 변형 공격 차단
사용자 정의 탐지룰 작성	관리자가 정규표현식(PCRE문법) 탐지룰을 직접 작성하여 입력 가능
공격 유형별 탐지룰	공격 유형, Application 별로 차단 가능 - 공격유형 : ActiveX, Scan, URL Attack... - Application : Database, SQL, OS, P2P, 메신저
Anomaly 탐지룰	다양한 이상 징후 공격에 대한 차단 탐지룰 지원
행위 기반 탐지	Agent Software를 이용하여 단말의 행위를 분석하여 공격 차단

〈Soligate RxIPS 공격 탐지룰〉



Routing

별도의 라우터나 L3 스위치 없이 라우팅 기능을 수행합니다.

✓ 특징
- 외부와 내부를 연결해주는 게이트웨이 역할 (L3 스위치 기능)

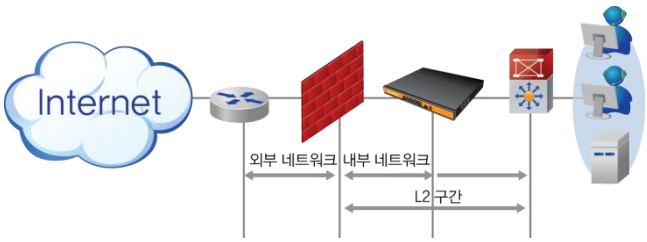
✓ 장점
- 다수의 LAN 포트를 이용하여 사용자 그룹 및 Server Farm의 물리적 구분

Bridge

기존 네트워크 구성 변경을 원하지 않으시는 고객에게는 Bridge 구성이 적합합니다.

✓ 특징
- 기존 네트워크 변경 없이 구성 가능

✓ 장점
- IPS, 유해사이트차단, 스팸 필터 등의 보안 기능 적용



Bypass

단일 구성에서 보안 장비의 링크 또는 전원 등의 문제가 발생하였을 경우에도 bypass 기능을 사용하여 네트워크 트래픽에는 영향이 없습니다.

✓ 특징
- 보안 장비 이상시에도 네트워크 정상 사용 가능

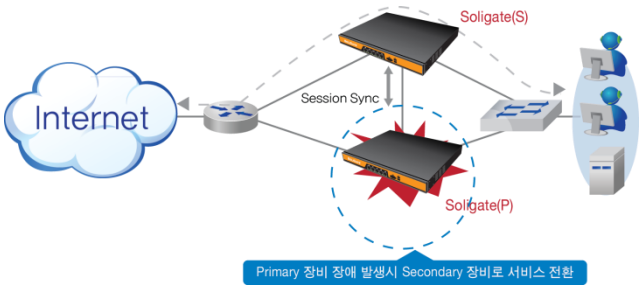
✓ 장점
- 서비스 가용성 보장

HA(High Availability)

중단 없는 네트워크를 위해 이중화 구성이 가능합니다.

✓ 특징
- Active-Active, Active-Standby 구성 가능
- 장비 간 설정 및 상태 정보 공유
- 별도의 L4 장비 없이 로드밸런싱 수행

✓ 장점
- 장비 장애 시 자동 전환
- 서비스 가용성 보장



침입 탐지 및 방어 시스템(IPS : Intrusion Prevention System)

인프니스네트웍스 Soligate RxIPS는 네트워크와 시스템에 대한 비정상적인 패킷과 세션을 차단하는 기능은 물론, 다양한 형태의 침입 행위에 대해 즉각적으로 탐지하고 분석하여 능동적으로 대응합니다.

Deep Packet Inspection

Soligate RxIPS의 IPS 엔진은 강력한 침입 탐지 및 방어 기능을 수행합니다. 3,000여 개의 알려진 공격에 대한 최신 시그너처로 웜, 바이러스, 악성 코드를 차단합니다. 또한 SQL Injection, Web Shell Upload, 애플리케이션 취약점을 이용한 Exploit 코드와 같은 다양한 형태의 공격을 방어합니다.

정규표현식(PCRE) 전수조사

Soligate RxIPS는 정규표현식 전수조사 기술을 지원하여 변형된 공격을 차단합니다. 관리자가 정규표현식 패턴을 변형하지 않고 직접 입력이 가능하며 3,000개 이상의 패턴을 적용하여도 성능 저하가 미미합니다. 표본조사가 아닌 전수조사를 지원합니다.

DDoS(Distributed Denial of Service) 방어

Soligate RxIPS는 Ping of Death, LAND Attack과 같은 DoS 공격을 차단합니다. 또한 다양한 형태의 Flooding 공격을 차단하는 기능을 제공합니다. SYN, ACK, RST, URG 등의 TCP flooding 공격을 방어하고, UDP, ICMP flooding 및 DNS query 공격 등도 차단합니다.

침입 차단 시스템(Firewall)

외부와 내부의 접점에서 보안 게이트웨이 역할을 수행합니다. 안전한 환경(DMZ)을 구성할 수 있습니다.

상태기반 감시(Stateful Inspection)

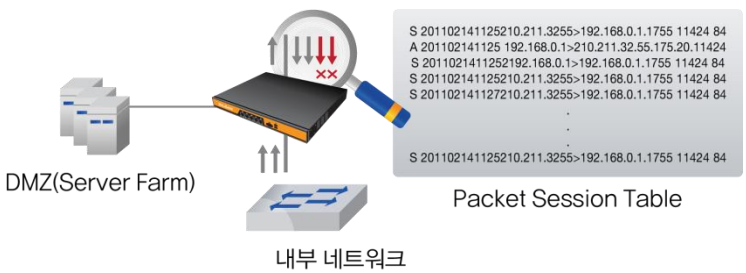
Soligate RxIPS는 일정 시간 동안 통신 패킷을 추적함으로써 강화된 보안 기능을 제공합니다. 송수신 패킷을 모두 검사하며, 특정한 형태의 수신 패킷을 요청하는 송신 패킷들도 추적하여 오직 적절한 응답이라고 판단되는 수신 패킷에 대해서만 통과를 허용합니다. 즉, 관리자가 정의한 보안 정책에 적합하도록 패킷의 상태 정보를 이용하여 좀더 빠르고 높은 보안성을 제공합니다.

L2 기반 차단 기능 제공

ARP 프로토콜의 취약점을 이용하는 ARP Spoofing 공격, IP 프로토콜의 인증 취약점을 이용하는 IP Spoofing 공격 등의 차단 기능을 제공합니다.

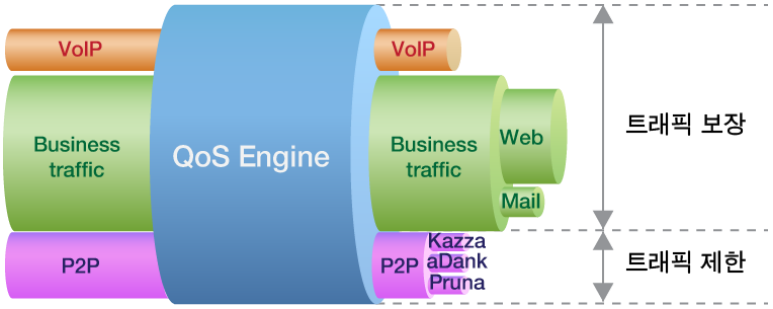
NAT

1:1, N:1, M:N 등 다양한 NAT 환경을 지원합니다.



품질 보장 서비스(QoS : Quality of Service)

QoS 기능은 트래픽 관리를 위한 기능입니다. 대용량 대역폭의 회선을 사용한다고 해도 P2P와 같은 하나의 프로그램이 전체 대역폭을 점유할 수 있습니다. Soligate RxIPS는 트래픽을 보장 또는 제한합니다.



- ✓ 업무용 또는 중요 트래픽 보장
- ✓ P2P와 같은 비업무 트래픽 제한
- ✓ IP, 포트별 제어
- ✓ 사용 그룹별, 시간별 적용 가능
- ✓ Shaping 방식으로 데이터 무손실

유해 컨텐츠 차단

유해 사이트 차단

Soligate RxIPS는 관리자가 정의한 정책에 따라 업무와 연관성이 없는 웹 사이트 접근을 차단합니다. 방송통신심의위원회에서 제공하는 DB와 연동하여 유해사이트 차단 정책의 설정이 가능합니다. 또한 내용등급(PICS label) 표시에 따른 차단 기능을 제공합니다. P2P, 웹하드, 게임 사이트 등의 유해 사이트 목록을 항목별로 분류하여 제공합니다. 사용자 정의 URL filter 기능은 관리자의 판단에 따라 특정 웹 사이트를 차단할 수 있도록 합니다.

웹 메일 차단

Web Mail Filter 기능은 내부 정보가 외부로 허락없이 유출되거나, 외부의 감염 데이터가 분별없이 내부망으로 침입하는 경로를 차단하는 것이 목적입니다. 관리자가 정의한 정책에 따라 지정된 웹 메일 서비스의 읽기, 쓰기, 파일 첨부 등의 기능을 제한할 수 있습니다.

스팸 차단

스팸 차단 기능은 내부망으로 전송되는 메일의 내용과 첨부 파일을 검사하여 스팸 메일인 경우 격리 처리합니다. 격리된 메일은 운용 방식에 따라 파기하거나 임시로 저장해 둘 수 있습니다. 더불어 2,381,093개의 바이러스 시그너처와 비교하여 메일과 첨부 파일의 바이러스 감염 여부를 판단하고 감염된 메일은 차단합니다. 또한, 메일 크기를 제한할 수 있는 기능을 제공합니다.

관리 기능

관리자는 직관적인 사용자 인터페이스를 사용하여 다양한 보안 정책을 설정할 수 있습니다.

모니터링 및 로그 검색

장비 상태, 보안 이벤트의 실시간 모니터링 및 로그 검색 기능을 제공하여 각종 보안 사고를 예방할 수 있습니다.

- ✓ CPU 부하량 모니터링
- ✓ 메모리/디스크 사용량 모니터링
- ✓ 실시간 보안 로그 모니터링 및 로그 검색 기능

INFNIS

㈜인프니스네트웍스

서울시 강남구 논현동 130-29 (논현로 653) 3층
http://www.infnis.com
TEL 02-3443-3456 (代)
FAX 02-3443-6060
E-mail sales@infnis.com