AhnLab

Case Study

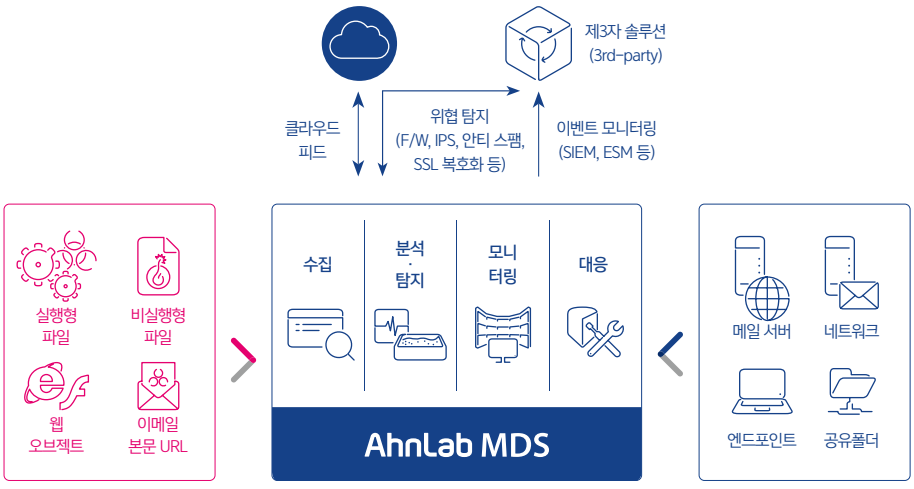
도입 사례로 살펴보는 AhnLab MDS 활용법

안랩의 APT 솔루션 AhnLab MDS는 네트워크/이메일/엔트포인트 간 유기적 연계를 통해 지능형 위협 방어

개요

지능형 위협은 기존의 보안 위협과 달리 단일 보안 소프트웨어나 보안 장비만으로는 대응이 어렵다. 이와 같은 공격에 효과적으로 대응하기 위해서는 최신 공격의 특성을 다각도로 고려하면서도 기존 보안 솔루션과 유기적으로 연계된 사이버 킬체인(Cyber Kill-Chain)에 따라 공격 유입 경로별 최적화된 대응 방안이 필요하다.

이러한 지능형 위협 대응에 효과적인 솔루션이 AhnLab MDS(이하 MDS)다. 샌드박스 기반의 지능형 위협 대응 솔루션 MDS는 독자적인 기술의 멀티엔진을 이용해 고도화된 지능형 위협을 정밀하게 탐지한다. 직관적인 위협 가시성과 '수집-분석·탐지-모니터링-대응' 프로세스를 기반으로 네트워크와 엔드포인트 레벨의 유기적인 대응을 제공해 다양한 경로를 통해 유입되는 지능형 위협을 효과적으로 차단한다.



[그림 1] AhnLab MDS 개념도

대기업 환경 고려사항

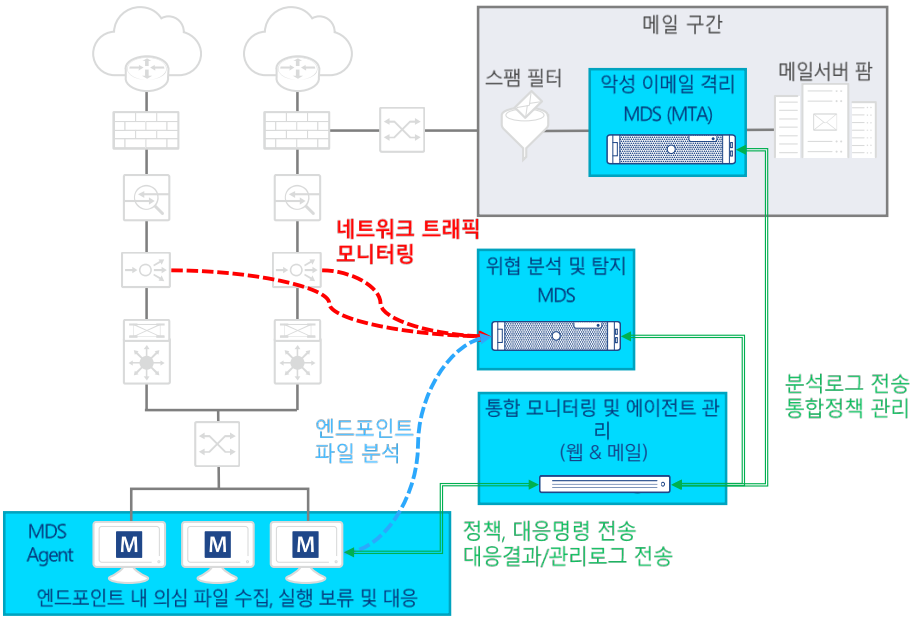
- 10G 이상 대역폭에서 다수 구간 모니터링 필요
- 대량 메일 실시간 분석 및 격리 필요

AhnLab MDS는 이미 여러 기업과 기관에서 지능형 위협 대응 솔루션으로 활용하고 있으며, 다양한 구축 사례를 통해 고객사의 IT 환경과 조직 문화에 따라 유연하게 구성하고 최적화된 정책으로 운영할 수 있도록 지원하고 있다.

이번 글에서는 조직의 규모와 특성에 따라 AhnLab MDS를 어떻게 구성하고 운영하고 있는지 도입 사례를 통해 살펴본다.

대기업 도입 사례: 보안성과 효율성 '일거양득'

먼저 일정 수준 이상의 조직 규모를 갖춘 대기업 환경에 제안되는 AhnLab MDS(이하 MDS) 구성을 알아보자.



[그림 2] 대기업 환경에 구성된 MDS 구조

대기업 IT 환경의 특징을 살펴보면, 네트워크에서 10G급 이상의 대역폭에서 다수 구간의 모니터링이 필요로 한다. 이메일 구간도 대량 메일을 실시간 분석하고 악성 메일을 즉시 격리하기 위한 메일 전용 솔루션 구성이 고려되어야 한다.

이에, 고객의 네트워크 환경 분석을 진행해 최적화된 미러링 구간을 찾고, 여러 대의 MDS 분석 솔루션을 구성해 네트워크로 이동하는 파일 및 패킷을 분석한다.

대기업 도입사례

- 다수 MDS와 MDS Manager를 통해 네트워크, 이메일, 엔드포인트 구간에서 발생한 공격들을 유기적으로 분석하고 통합 관리

이메일의 경우, MDS(MTA 라이선스)를 메일 구간에 별도로 구성하고 스팸 솔루션에서 1차 필터링된 메일을 전달받아 전수 검사를 진행한다. 악성 메일은 메일 서버로 전달하지 않고 MDS 솔루션 자체에 직접 격리하고 정상 메일만 메일 서버로 전달한다. 선 격리 조치 후 수신자 계정으로 메일 격리 사유를 안내하는 경보 메일을 발송하기 때문에 분석 완료 전에 사용자의 실수로 첨부파일이나 링크를 클릭해서 발생할 수 있는 사고를 방지할 수 있다.

사용자 PC도 다양한 환경에서 대규모로 운영되기 때문에 각 업무에 따라 별도 정책을 운영할 수 있도록 지원한다. 인사 연동을 통해 부서별 예외 정책 관리도 가능하다.

[그림 2] 구조도에 있는 'MDS Manager'는 네트워크, 이메일, 엔드포인트의 다양한 구간에서 수집되어 분석이 완료된 로그와 악성 공격의 실시간 대응 결과, 에이전트 상태 등을 통합 모니터링 할 수 있는 솔루션이다. 운영자는 MDS Manager에 접속해 다수 MDS 분석 솔루션의 하드웨어 리소스 정보와 샌드박스 분석에 대한 실시간 모니터링 현황을 확인할 수 있다.

그 외에도 운영에 필요한 다양한 예외 정책을 여러 MDS에 각각 설정하지 않고, MDS Manager에서 일괄 적용하거나 그룹별로 MDS를 분리하여 정책을 적용하는 기능도 지원한다. 결론적으로 고객은 다수 MDS와 MDS Manager를 효율적으로 운영해 대량의 네트워크, 이메일, 엔드포인트 구간에서 발생한 공격들을 유기적으로 분석하고 통합 관리할 수 있게 된다.

중견기업 도입 사례: MDS 1대로 견고한 보안 구축

중견기업 구성의 경우, MDS 1대로 네트워크, 메일, 엔드포인트 주요 구간을 모니터링하고 실시간 대응이 가능하도록 되어 있다. MDS는 HTTP, FTP, SMB, 이메일 등 다양한 프로토콜 분석이 가능하기 때문에 전체 구간에 유입되는 위협에 대해 단일 솔루션 구성으로 대응한다.

네트워크 구간에서는 본사의 이중화된 백본과 주요 자산으로 분류되는 서버팜을 실시간으로 모니터링 하면서, 사용자 PC의 악성 사이트 접속과 외부에서 시도하는 악성 네트워크 행위를 모니터링 하고 실시간 차단한다.

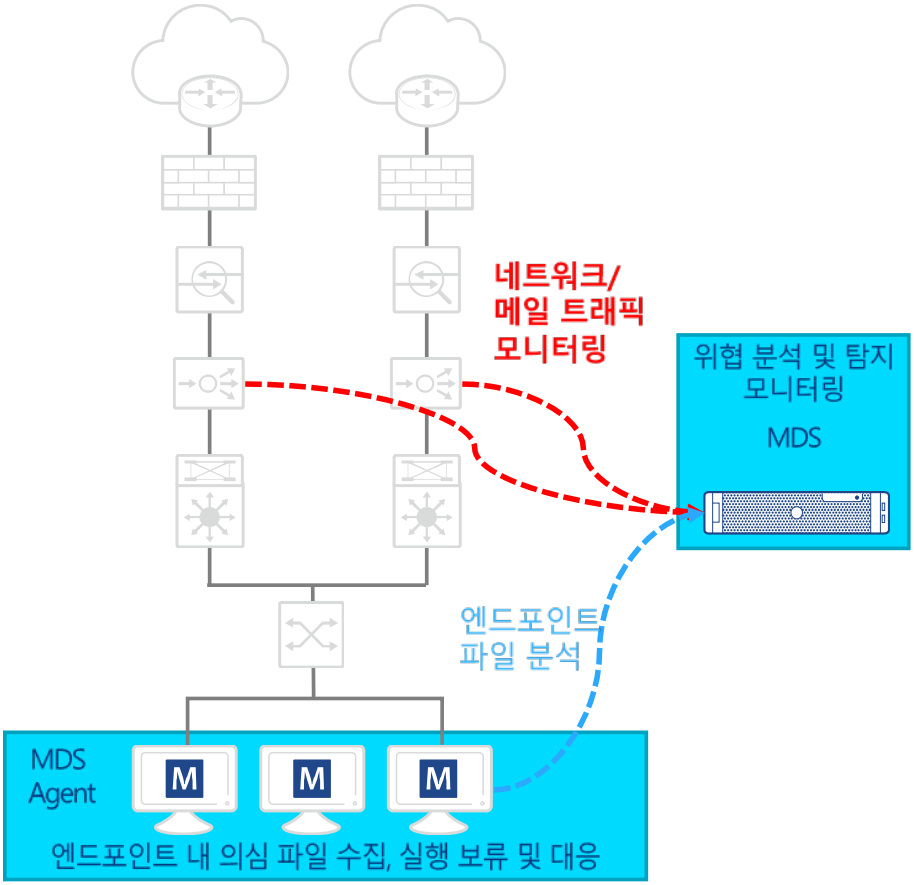
이메일 구간은 안티스팸 솔루션과 메일 서버 구간 네트워크 미러링을 통해 SMTP, POP3 등 다양한 메일 프로토콜의 트래픽에서 메일 데이터를 수집한다. 메일 서버로 유입되는 메일 본문과 첨부파일에 대해 솔루션이 실시간 분석을 진행한다. 악성 또는 악성 의심 메일이 확인될 경우에는 MDS에서 메일 수신자 계정으로 경보 메일을 자동 발송한다. 자동 발송되는 경보메일을 통해 발신자, 수신시각, 악성 메일 정보를 전달하여 사용자가 메일함

중견기업 도입사례

- MDS 1대로 네트워크, 메일, 엔드포인트 주요 구간을 모니터링하고 실시간 대응

의 악성 의심 메일을 즉시 삭제하도록 한다.

엔드포인트 구간에서는 MDS Agent가 동작하며, 실시간 감시를 통해 네트워크, 이메일, USB 등 엔드포인트로 유입되는 악성코드를 자동 분석한다. 악성으로 확인될 경우 차단 및 삭제하여 감염을 사전에 차단한다.



[그림 3] 중견기업 환경에 구성된 MDS 구조

이와 같은 구성은 단일 MDS 솔루션으로 주요 구간을 전부 모니터링하고 대응 기능도 활용 가능해 저비용 고효율의 효과를 발휘한다. 단일 솔루션 구성은 에이전트 관리 성능을 고려했을 때 5000대 이하의 PC 환경에 적합하다. 그 이상의 규모로 구성된 환경에서는 에이전트 관리를 위해 별도 MDS Manager 추가 구성이 필요하다.

금융/공공기관 도입 사례: 망분리 환경에 적합한 구성

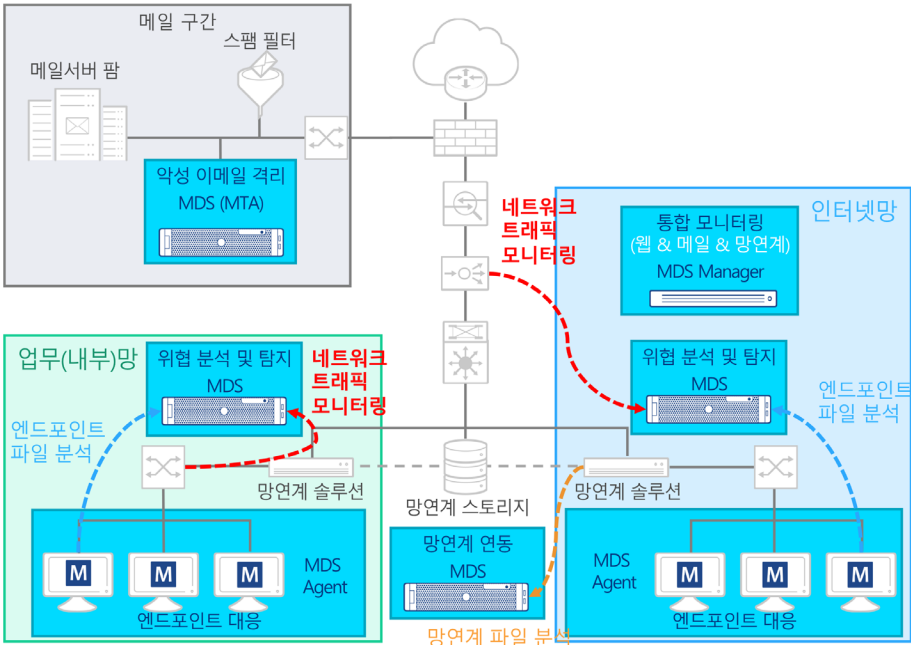
금융 및 공공기관의 경우는 망분리 환경을 고려해 MDS 솔루션을 구성한다. 인터넷망과

금융/공공기관 도입사례

- 인터넷망과 업무망에 각각 MDS 분석 솔루션을 별도로 구성
- 망연계 솔루션과의 연동을 통해 망간 이동되는 파일에 대한 전수검사 지원

업무망에 각각 MDS 분석 솔루션을 별도로 구성하고, 망연계 솔루션과의 연동을 통해 망간 이동되는 파일에 대한 전수검사도 지원한다.

통합 모니터링 및 관리를 위한 MDS Manager를 필요 시 인터넷망과 업무망에 각각 구성하여 망분리 정책에 위배되지 않게 운영한다. 이처럼 MDS는 망분리 네트워크와 이메일, 엔드포인트 구간에 망연계 솔루션 연동까지, 모든 구간에서 빈틈없는 탐지와 대응이 가능하도록 구성된다.



[그림 4] 금융/공공기관 환경에 구성된 MDS 구조

망분리 환경은 일반 기업 네트워크와 비교했을 때, 한쪽은 인터넷망, 다른 쪽은 업무망(폐쇄망) 환경이기 때문에 솔루션을 운영하는 방법에도 차이가 있다. 인터넷망은 클라우드 실시간 연결을 이용한 평판 정보를 분석에 활용하고, 업무망에서는 수동 엔진 업데이트와 샌드박스 내 가상 네트워크 분석 환경을 통해 분석 기술을 다양화하고 있다.

다음으로 활용 사례 별 MDS 구성 방안에 대해 살펴보자.

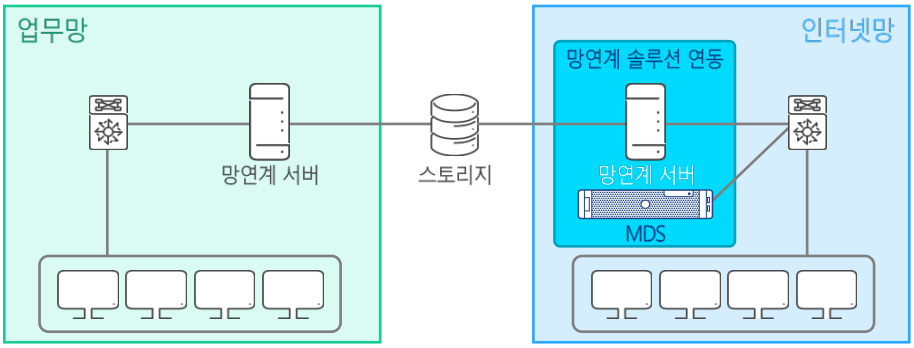
활용 사례 1: 망연계 구성

망연계 구성은 망연계 솔루션 종류에 따라 2가지 연동 방식을 지원하고 있다.

망연계 구성 사례

- 공유폴더 연동: 공유폴더를 실시간 감시하고 분석 결과를 전달해 악성파일 차단
- API 연동: 망간 전송 파일을 분석해 결과를 망연계 솔루션에 회신

먼저, '공유폴더 연동'은 망연계 솔루션 디스크 영역에 공유폴더를 생성하고, 파일을 망간 이동시키기 전 공유폴더로 복사해 놓는다. MDS 솔루션은 공유폴더를 실시간 감시하면서 복사된 파일이 확인되면 이를 분석하고 망연계 솔루션으로 결과를 전달한다. 정상파일을 제외한 악성파일은 전송되지 않도록 망연계 솔루션에서 차단한다.



[그림 5] MDS 망연계 구성

다음으로 'API 연동'은 망간 전송되는 파일을 망연계 솔루션에서 RestAPI 호출을 통해 MDS로 파일 분석을 요청한다. MDS에서는 전달받은 파일을 분석해 분석 결과와 상세 분석 리포트를 망연계 솔루션으로 회신한다.

MDS는 대부분의 국내 망연계 솔루션과 이 두 가지 방법으로 이미 연동 개발이 되어 있기 때문에, 공유폴더 혹은 API 연동을 통해 망연계 구간의 MDS 연동 구축을 단기간에 완료할 수 있다.

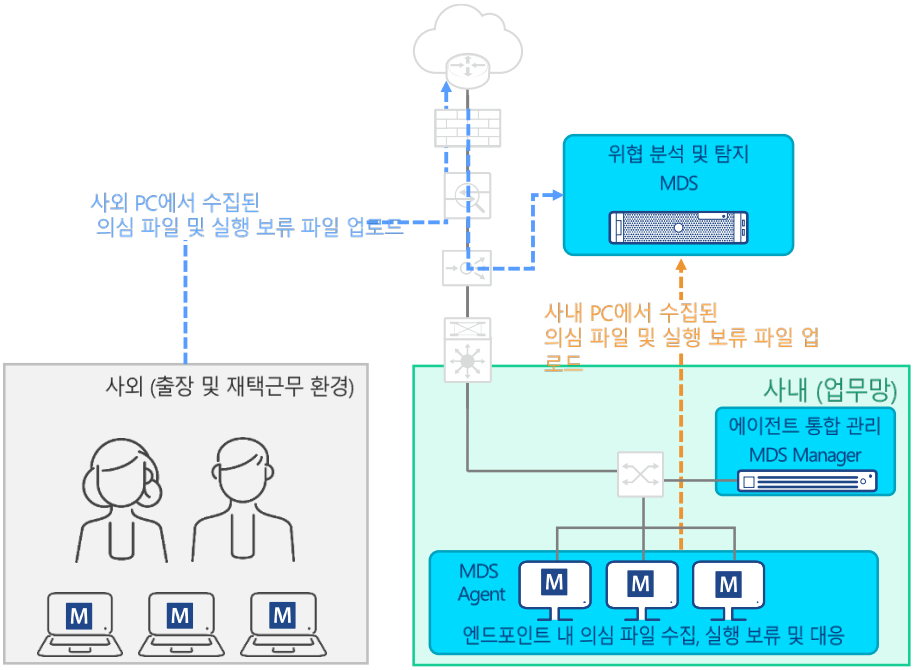
활용 사례 2: 엔드포인트 단말 분석

고객사에 상황에 따라 엔드포인트 단말 분석을 위한 구성으로만 MDS를 도입하는 경우도 있다. 이는 네트워크 장비들이 분산되어 있어 중앙 관리되는 미러링 구성이 힘든 경우, 또는 MDS가 아닌 다른 종류의 솔루션을 이미 네트워크에 구축해서 사용중인 경우이다.

다른 솔루션을 통해 네트워크 구간 모니터링을 하고 있지만, 에이전트가 없어 감염을 확인한 이후, PC 포맷 혹은 수동으로 PC를 점검하는 등 추가 업무로 인해 운영자와 사용자 모두 불편함을 겪는 사례가 많아지고 있다. 이를 해결하기 위해 악성코드 실시간 대응과 엔드포인트 보안 강화를 목적으로 MDS를 도입하여 자동화된 대응 기능을 효과적으로 사용하고 있다.

엔드포인트 단말 분석 사례

- 네트워크 장비 분산, 혹은 다른 솔루션을 이미 네트워크에 구축/사용중인 경우
- 자동화된 대응 기능으로 엔드포인트 보안 강화
- 사외 단말에서 사내와 동일한 수준의 보안 유지



[그림 6] MDS 엔드포인트 단말 분석

특히, 코로나19로 재택근무가 일반화되면서, MDS Agent의 강점 중 하나인 사외 단말에 대한 분석 지원 기능을 통해 사외 환경에서 사내와 동일한 보안을 유지하는 방안으로도 활용되고 있다. MDS에 NAT(Network Address Translation)된 공인 IP를 할당하여 사내·사외 구분 없이 지원하는 방안이 있으며, 금융권과 같이 망분리 환경의 경우 DMZ 구간과 업무망 구간에 MDS를 각각 구축한다. VPN 접속 이전에는 MDS를 통한 DMZ 구간 대응, VPN 접속 이후에는 업무망 구간의 MDS를 통해 엔드포인트 위협 대응이 가능하도록 MDS Agent에서 자동 스위칭 기능을 지원한다.

이와 같은 구성은 금융권과 기업에서 재택근무 관련 사외 환경의 PC 신·변종 악성코드 감염 대응 방안으로 도입하는 사례가 지속적으로 증가하고 있다.

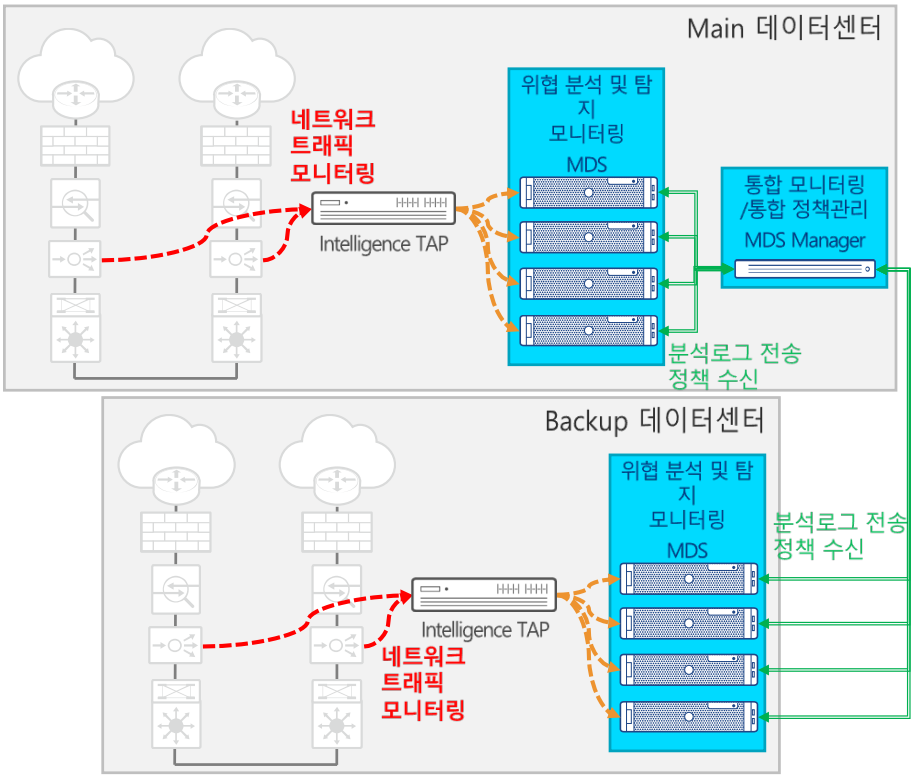
활용 사례 3: 그룹사 네트워크 모니터링

그룹사 환경에서 네트워크 관제를 지원해야 하는 경우, 메인 IDC(Internet Data Center)와 DR(Disaster Recovery) 데이터 센터에 인텔리전스 TAP(Test Access Point)와 다수의 MDS를 통해 각 MDS 솔루션 별로 트래픽을 분산해 수집할 수 있도록 구성하고 있다.

그룹사 네트워크 모니터링 사례

- 네트워크 관제 시 각 MDS 솔루션별로 트래픽을 분산해 수집할 수 있도록 구성
- 각 MDS에서 분석된 로그는 MDS Manager를 통해 한 번에 관리

각 MDS에서 분석된 로그는 MDS Manager를 통해 한 번에 관리 가능하기 때문에 수십 대의 MDS 솔루션도 불편함 없이 관제 조직에서 통합 관리가 가능하다. 안랩은 다년간의 기술지원 노하우와 지속적인 기능 개선을 통해 그룹사 관제에서 필요로 하는 최적화된 다양한 부가 기능도 지원하고 있다.



[그림 7] MDS 그룹사 네트워크 모니터링

활용 사례 4: 그룹사 이메일 모니터링

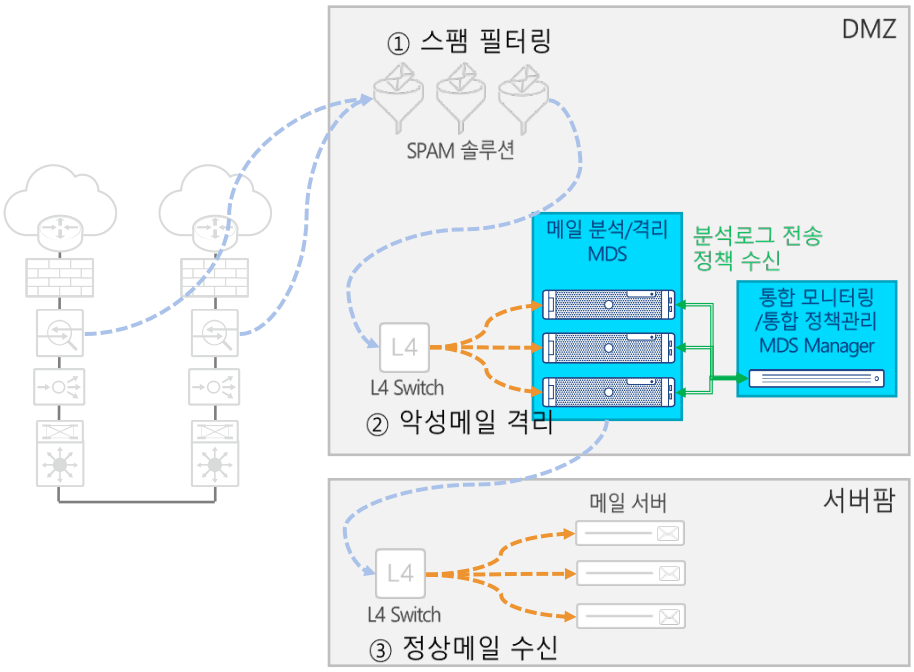
그룹사 이메일 모니터링 역시 MDS 구성으로 지원이 가능하다.

안티스팸 솔루션과 메일 서버팜 사이에 L4 스위치, 하위에 Virtual IP로 관리되는 다수 MDS 솔루션을 구축하여 부하 분산(load balancing)된 환경에서 장애 없이 신속한 메일 분석을 지원한다.

MDS Manager에서 모든 분석 결과를 통합관리 할 수 있어 다수 솔루션으로 구성된 환경에서도 자동화된 이메일 분석과 격리 결과 실시간 검색이 가능하다. 또한, 격리된 이메일을 손쉽게 재전송하거나 추가 분석에 활용할 수 있다.

그룹사 이메일 모니터링 사례

- 다수 MDS 솔루션을 구축해 로드 밸런싱된 환경에서 신속한 메일 분석 지원
- 자동화된 이메일 분석, 격리 결과 실시간 검색, 격리된 이메일 재전송 및 추가 분석 활용 가능



[그림 8] MDS 그룹사 이메일 모니터링

결론

지금까지 조직 규모 별, 활용 사례 별로 MDS를 활용한 다양한 구성에 대해 알아보았다. 모든 네트워크 환경이 위에 설명한 환경과 100% 일치하지는 않으며, 조직의 특성에 따라 조금씩 다른 환경인 경우가 대부분이다. 안랩은 이미 많은 고객사에 MDS를 구축한 경험이 있기 때문에 이런 노하우를 바탕으로 네트워크 환경 분석 검토를 거쳐 가장 이상적인 구성을 제안한다.

한편, 안랩은 2021년 7월부터 MDS 솔루션 임대와 원격관제를 포함한 'MDS 관제 서비스' 제공을 시작했다. 월별 과금 체계를 통해 초기 솔루션 도입 부담을 낮출 수 있으며, 고객사 내부에 구축된 MDS를 통해 위협 이벤트를 탐지하게 되면, 24시간 원격관제시스템을 통해 실시간 위협 탐지 보고서를 메일로 발송한다.

전문가의 추가 분석이 필요한 경우 '악성코드 전문가 분석 서비스'도 이용 가능하다. APT 대응 솔루션 도입을 검토하고 있지만, 비용 문제나 보안 운영 인력의 부족을 이유로 고민하고 있다면 'MDS 관제 서비스'가 좋은 해답이 될 수 있다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901