기능 소개

보안 툴에 인라인 바이패스가 필요한 이유

네트워크 속도로 보안을 유지합니다.

인라인 바이패스: 애플리케이션 이중화를 높이고 보안 툴의 최대 성능을 확보합니다.

핵심 이점

- ✓ 인라인 보안 툴이 애플리케이션을 간섭하는 장애 지점으로 되지 않게 합니다.
- ✓ 보안 툴을 최대한 활용합니다.
- ✓ 효율성 및 확장 증가를 통해 ROI를 개선합니다.
- ✓ 애플리케이션이나 네트워크 작동 시간을 중단시키지 않고 보안 툴을 업데이트하거나 교체합니다.
- ✓ 공격을 받으면 툴을 감지 모드에서 초 단위로 인라인 차단 모드로 전환합니다.
- ✓ 새 보안 툴을 시험하여 생산 네트워크 트래픽과 비교합니다.
- ✓ 페일 투 와이어(fail-to-wire)의 물리적 바이패스 보호를 활용하여 전원 손실 시에도 네트워크 트래픽을 계속 가동합니다.

이중화, 성능, 보안, 비용의 최적화

웹 애플리케이션 방화벽(WAF), 침입 차단 시스템(IPS), 고급 위협 차단(ATP)과 같은 인라인 보안 툴은 네트워크 보안에 필수적이지만, 자체적인 문제를 일으킬 수 있는데, 예를 들면

- 이러한 툴이 네트워크 장애 요소가 된다는 것입니다.
- 인라인 툴이 전원을 잃거나, 소프트웨어 장애가 발생하거나, 유지보수를 위해 인라인 툴을 사용하지 않으면, 중요한 애플리케이션이 동작을 중단할 수 있습니다.
- 네트워크 트래픽이 피크 상태이고 보안이 대단히 중요할 때 인라인 툴은 애플리케이션 성능을 저하시키는 병목 현상이 될 수 있습니다.

다행히, 쉽게 배포할 수 있는 비용 효과적인 솔루션이 있습니다. 보안을 위해 특별히 개발된 차세대 네트워크 패킷 브로커인 기가시큐어® 보안 전달 플랫폼(기가시큐어)에서 찾아볼 수 있는 인라인 바이패스 기능을 소개합니다. 인라인 바이패스를 활용하면 어렵지 않게 다음과 같은 일이 가능합니다.

- 인라인 보안 툴이 단일 장애 지점으로 되지 않게 합니다.
- 보안 장치에 네트워크 트래픽을 효율적으로 배포하므로, 모든 네트워크 링크에 필요한 대형 시스템을 구매하는 데 드는 높은 비용을 피할 수 있습니다.

또한 네트워크 성능과 보안 사이에 스마트한 균형을 이룰 수도 있는데, 예를 들어

- 더 짧은 대기 시간이 대단히 중요한 트래픽을 우회하면서 고위험 트래픽 검사를 선택할 수 있습니다.
- 네트워크 대기 시간에 영향 미치지 않도록 대역 외 감지 모드에서 보안 툴을 배포하지만, 이후 공격 감지 시 악의적 활동을 실시간으로 차단하기 위해 인라인 보호 모드로 쉽게 전환할 수 있습니다.

트래픽 상시 가동

보안 툴은 때때로 정전, 소프트웨어와 하드웨어 장애, 유지보수, 교체로 인해 오프라인으로 전환됩니다. 기가시큐어는 양방향 하트비트 패킷을 활용하여 툴의 상태와 성능을 모니터링합니다. 이후 툴이 오프라인으로 전환되거나 네트워크 트래픽 급증에 휩싸이는 경우 기가시큐어는 툴을 우회하여 중요 애플리케이션 트래픽을 계속 가동시킵니다.

차세대 기능의 이점

인라인 보안 툴의 제한적인 트래픽 기능은 검사가 필요한 네트워크 트래픽 대역폭 이하로 떨어질 수 있습니다. 또한 네트워크가 10Gb에서 40Gb로 다시 100Gb로 진화함에 따라 그에 걸맞는 고속 인터페이스로 툴을 배포하는 경우 제한적인 예산의 문제에서 벗어날 수 있습니다.

여기에서도 기가시큐어는 보안 툴에 걸쳐 인라인 트래픽을 분산하는 역할을 합니다. 분산은 전반적인 검사 용량을 늘릴 뿐만 아니라 기존의 저속 툴을 확장하여 고속 네트워크를 보호함으로써 ROI를 향상시킵니다.

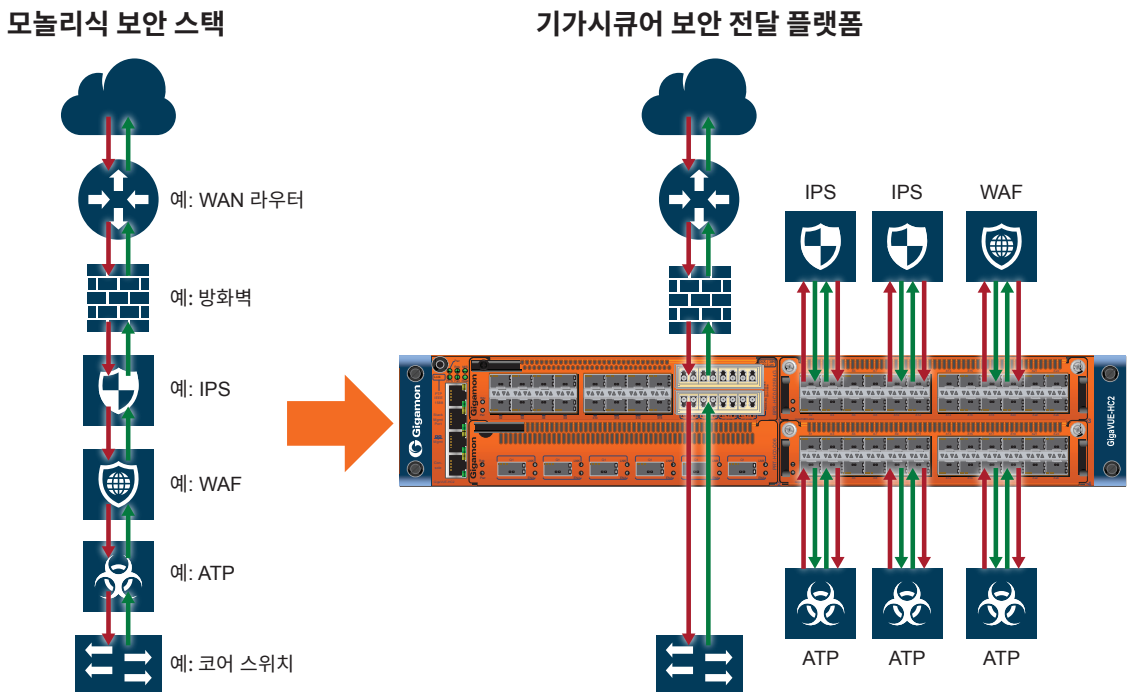

그림 1: 기가시큐어를 활용한 위협 차단 툴 확대

어떻게 작동할까요? 트래픽 분산 알고리즘은 하드웨어에서 라인 속도로 작동하고 각 툴이 최고의 효과를 위해 전체 양방향 세션을 볼 수 있게 합니다. 이 기능에는 이중화 기능이 탑재되어 있으며, 이를 통해 툴이 장애를 일으키거나 오프라인으로 전환될 때 시스템은 상태가 좋은 툴에 트래픽을 재분산합니다. 1+1 또는 N+1 이중화 기능을 통하여 보안과 네트워크 가용성을 훨씬 더 높일 수 있습니다.

보안 툴의 감지와 차단 모드 간 마이그레이션

기가시큐어는 대역 외 및 인라인 보안 툴 모두를 지원하므로 사용자가 보안과 네트워크 성능 모니터링을 위해 인라인 트래픽을 대역 외 감지 툴에 복제할 수 있습니다. 이 트래픽에서 기가시큐어는 메타데이터도 생성한 후 SIEM(보안 정보 및 이벤트 관리)뿐만 아니라 IPFIX 또는 CEF 기반의 데이터를 처리하는 다른 툴에도 이 메타데이터를 전송할 수 있습니다.

인라인 차단 툴은 대부분 대역 외 감지 모드에서도 작동할 수 있습니다. 기가시큐어 보안 전달 플랫폼은 인라인 트래픽 사본을 발송하여 감지 모드에 있더라도 툴 인라인을 배포하는 용도로 사용할 수 있습니다. 보안 툴이 인라인으로 이동할 준비가 되었을 때, 잘 알려진 스위치의 조작으로 트래픽을 인라인 툴로 직접 전송합니다. 다시 스위치를 조작하면 감지 모드로 다시 전환할 수 있습니다.

성능에 민감한 애플리케이션 환경에서는 종종 감지 모드에서 대역 외 보안 툴을 가동하는 것이 당연하기 때문에 네트워크 대기 시간에 영향을 미치지 않습니다. 위협이 해결될 때까지 툴은 멀웨어, 저해된 웹사이트에 대한 링크, 명령과 제어 트래픽을 차단할 수 있습니다.

간단한 보안 툴 업데이트, 배포, 테스트

기가시큐어 인라인 바이패스 기능을 활용하면 유지보수 기간 일정을 잡거나 애플리케이션에 대한 접근성을 중단하지 않고도 업데이트나 교체를 위해 툴을 오프라인으로 전환할 수도 있습니다.

또한 기가시큐어는 장치를 대역 외에서 초 단위로 인라인으로 전환할 수 있기 때문에 실제 네트워크 트래픽으로 보안 툴을 쉽게 테스트할 수 있습니다. 예는 다음과 같습니다.

- 감지 모드에서 업그레이드된 툴 유효성 검사
- 기본 정상 동작을 설정하여 네트워크를 모니터링하는 데 필요한 툴 교육

이후 준비 상태가 되면 순간적으로 툴을 인라인 모드로 다시 전환할 수 있습니다.

기가시큐어 인라인 바이패스에 대한 상세 학습

기가시큐어 보안 전달 플랫폼의 인라인 바이패스 기능이 네트워크에 어떻게 도움이 되는지를 알아보려면 **www.gigamon.com/gigasecure**를 참조하시기 바랍니다.

6116-01 04/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com