ciena
Experience. Outcomes.

애플리케이션 정보

클라우드 보안

Layer 1 암호화로 데이터 센터 간 보안 간소화

민감하거나 업무에 필수적인 데이터를 보호하는 것은 지적 재산과 기밀 기록을 보호하고 데이터 침해로 인한 벌금 및 재정 손실을 방지하는 데 매우 중요합니다. 하지만 어떤 데이터를 어떻게 보호할지 결정하는 것은 쉬운 일이 아닐 수 있습니다. 데이터 센터의 물리적 설계는 원치 않는 액세스를 제한하기 위해 여러 계층의 물리적 보안 조치를 통합하며, 방화벽, 바이러스 백신 및 침입 감지 기술은 데이터 센터 내에서 데이터의 보안을 유지하는 데 사용될 수 있습니다. 그러나 정보가 데이터 센터의 안전한 범위를 벗어나게 되면 정보의 보안은 종종 방치됩니다.

데이터 센터를 상호 연결하는 광 케이블 네트워크는 대개 공격의 영향을 받지 않는 것으로 생각되어 왔지만 데이터 센터 간 통신을 무시하면 하나의 데이터 센터에서 다른 데이터 센터 내 애플리케이션 또는 장치로 민감한 데이터가 전송될 때 취약성이 발생합니다. 데이터가 조직의 제어 범위를 벗어난 링크를 통과할 수 있으므로 노출 및 손상될 위험이 있습니다.

조직에서는 데이터 센터 내에서뿐만 아니라 데이터 센터 간에 이동할 때 애플리케이션과 정보의 보안을 유지해야 합니다. 데이터 센터 간 보안은 설계, 구현 및 확장하기 어려울 수 있습니다. 애플리케이션 계층 암호화는 데이터 센터 간 상호 연결의 보안을 유지할 수 있습니다. 패킷 계층 암호화도 도움이 될 수 있지만 유형마다 고유한 해결 과제가 있습니다. 세 번째, 보다 매력적인 옵션은 최하위 네트워킹 계층, 즉 광 계층에서 네트워크 데이터를 암호화하는 것입니다. 대규모 광 계층 암호화는 아키텍처 확장성, 엔지니어링 간소성 및 운영 편의성을 지원하는 동시에 데이터 센터 간에 전달되거나 클라우드를 통과하는 모든 전송 중 데이터를 보호합니다.

매우 중요한 데이터 센터 간 네트워크 보안

최근 연구에서 4개 조직 중 하나 꼴로 향후 24개월 이내에 대규모 데이터 침해를 경험할 수 있는 것으로 확인했습니다.[1] 데이터 침해 시 피해자를 식별하고 통지해야 하며 연관된 모든 법적, 규제적 요금을 지불해야 하므로 관련 비용은 수백만 달러에 이를 수 있습니다. 또한 데이터 침해가 발생하면 재정 손실 및 고객 이탈 그리고 조직의 평판 훼손 등을 통해 추가 비용이 발생할 수 있습니다.

Layer 1 암호화의 장점:

- 트래픽 정체 없는 전체 속도 처리량
- 뛰어난 데이터 센터 간 통신 보안을 위한 초저 지연 시간 회선 속도 암호화
- 추가 암호화 어플라이언스가 필요 없는 구축 및 운영이 간편한 솔루션
- 다양한 서비스를 위한 프로토콜 제약 없는 유연한 암호화

1 Ponemon Institute, "2017 Cost of Data Breach Study," Ponemon Institute Research Report(2017년 6월), 1-2

보안 침해에 대한 보다 엄격한 식별 및 통지를 요구하도록 법률이 점점 강화되고 있습니다. 전송되는 데이터 또는 기록의 유형에 따라 데이터 암호화를 요구하는 규제가 있을 수도 있습니다. 기업은 전체 수익성에 영향을 줄 수 있는 민감한 데이터가 유출된 경우 막대한 벌금에 직면할 수 있습니다.

보안에 대한 새로운 사고 방식 조성

보안을 고려할 때 조직에서는 침해가 발생할 수 있고 발생할 것임을 가정하는 새로운 사고 방식을 도입해야 합니다. 방어 수단이 공격자를 네트워크 외부에 유지할 것이라고 가정하는 것은 바람직하지 않습니다. 대신, 기업은 공격자가 이미 내부에 있거나 곧 내부로 침투할 것이라고 가정해야 합니다. 침해를 가정한 사고 방식을 도입하면 침투 방지 시스템을 설계하려고 애쓰거나 시스템이 노출된 후 데이터 보호를 걱정하는 대신 데이터를 항상 보호할 수 있는 방어 수단을 설계할 수 있습니다. 예를 들어 조직에서는 네트워크를 통해 전송 중인 데이터를 암호화할 수 있으므로 공격자는 전송 중인 데이터를 캡처할 수 있는 경우에도 이를 읽을 수 없습니다.

공격이 성공하려면 동시에 충족되어야 하는 몇 가지 핵심 구성 요소가 필요합니다. 패치가 적용되지 않은 소프트웨어와 같은 일부 약점이 내포된 취약한 시스템이어야 합니다. 공격자에게 가치가 있어야 하며 액세스할 수 있어야 합니다. 이 경우 공격자에게 적절한 도구와 기술이 있다면 침해가 발생할 수 있습니다.

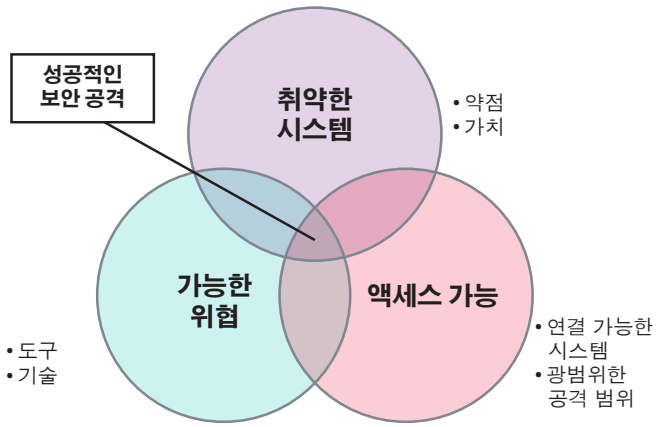

그림 1. 보안 공격을 성공으로 만드는 요소

방어 전략을 수립하려면 자산 식별, 액세스 권한 결정 및 위협 이해라는 세 단계를 수행해야 합니다. 자산을 식별할 때 조직에서는 중요한 자산(예: 데이터 및 기밀한 기록)이 무엇이며 이러한 자산이 어떻게 보호되고 액세스되는지 알아야 합니다. 데이터베이스 내의 데이터는 데이터베이스에 적용된 보호 기능으로 인해 보안이 유지될 수 있지만 이 데이터를 데이터베이스에서 내보낸 다음 네트워크 내로 이동하는 경우에는 더 이상 보안이 유지되지 않을 수 있습니다. 예를 들어 인사 부서에서 보고를 위해 데이터를 Excel로 내보내는 경우 데이터 센터 간에 암호화되지 않은 상태로 이동하는 스프레드시트 백업은 보안이 유지되지 않습니다.

포괄적인 보안 전략을 위해 네트워크 암호화 추가

포괄적인 보안 전략의 일환으로, 클라우드를 포함하여 데이터 센터 간에 모든 데이터를 보호하는 것이 무엇보다 중요합니다. 네트워크의 어떤 부분도 해킹의 영향을 받지 않을 것이라고 가정해서는 안 되며, 전송 중 데이터를 방치하는 것은 바람직하지 않습니다. 데이터 기밀성을 유지하기 위해 기업은 클라우드를 통해 전송되는 데이터의 보안을 유지할 수 있는 효율적이고 확장 가능한 방법을 포함하는 포괄적인 IT 보안 접근법을 도입해야 합니다.

기존에 IT 조직은 보안을 온-프레미스 보안, 즉 데이터 센터 진입점에서의 물리적 보안과 서버 및 장비에 대한 액세스 제한과 같은 요소를 포함하는 보안과 연관지었습니다. 방화벽, 침입 방지 시스템, 전체 디스크 암호화, 애플리케이션 및 데이터베이스 강화, 역할 기반 액세스 제어 및 기타 보안 요소는 중요한 데이터 저장소를 암호화하고 보안을 유지합니다. 그러나 데이터가 이러한 보안 구역 외부로 이동하거나 데이터 센터 간에 전송 중인 경우에는 공격과 침해에 취약할 수 있습니다. 게다가 타사 네트워크 또는 여러 서비스 공급자 네트워크를 통과하는 데이터는 단일 조직의 완전한 제어 범위 내에 있지 않을 수 있으므로 해당 보안을 유지하는 것이 더욱 까다로워집니다.

암호화는 데이터 센터 간에 전송되는 데이터를 보호하는 데 사용될 수 있지만 다양한 솔루션을 고려해야 합니다. 암호화 솔루션마다 고유한 장점과 난제가 있으므로 최상의 솔루션은 구축 및 관리가 용이하고 확장성이 뛰어나며 효율적이어야 합니다.

애플리케이션 계층 또는 네트워크 인프라 보안

암호화 솔루션을 구현할 때 IT 조직은 일반적으로 애플리케이션 계층을 보호하거나 네트워크 인프라에 내장된 암호화를 사용하려고 합니다. 애플리케이션 계층 보안은 호스트 장치와 애플리케이션 모두의 보안을 유지해야 하므로 대부분의 애플리케이션 계층 보안 프레임워크는 데이터 센터 내에 포함되어 있습니다. 또한 애플리케이션(예: 웹 브라우저 또는 이메일 클라이언트)과 서버 간의 통신 보안을 유지하는 TLS(전송 계층 보안)와 같은 솔루션은 일반적으로 클라우드를 통하거나 데이터 센터 간에 이루어지는 통신에 대한 애플리케이션 간 보안을 다루지 않습니다. 여러 데이터 센터 전반의 애플리케이션 간 보안을 위한 공통 프레임워크를 구축하는 것은 까다로울 수 있으므로 조직에서는 대부분 네트워크 인프라를 통해 솔루션을 찾으려고 합니다.

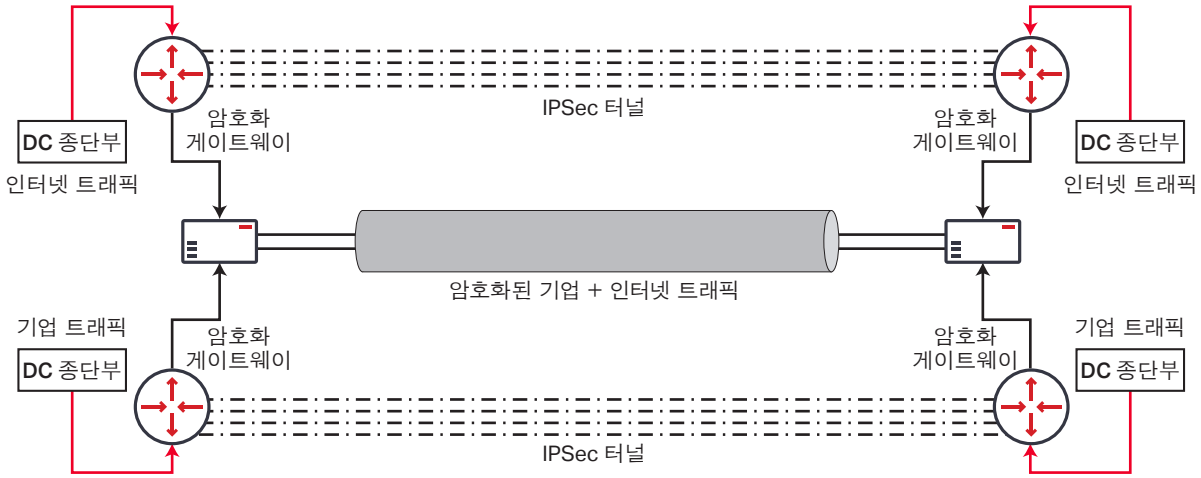

그림 2. 오버레이로 패킷 계층에서 모든 트래픽 보안 유지(논리 뷰)

네트워크 인프라 사용에는 고유한 해결 과제가 따르며, 인프라 계층에서 네트워크 보안을 유지하면 네트워크 아키텍처가 매우 복잡해질 수 있습니다. 데이터 센터 간의 트래픽 흐름이 매우 크기 때문에 여러 100G+ 연결에 걸쳐 모든 트래픽의 보안을 유지하는 것은 운영이 까다롭고 설계와 확장이 어려울 수 있습니다.

한 가지 옵션은 암호화된 VPN 게이트웨이 오버레이를 사용하여 패킷 계층에서 트래픽의 보안을 유지하는 것입니다(그림 2). 이를 위해서는 보호가 필요한 각 링크에서 전문화된 고가의 암호화 게이트웨이 장비를 사용해야 합니다. 이 모델은 트래픽을 단일 소스/대상 IP 쌍으로 제한하며, 가장 바깥쪽 IPsec 헤더 정보를 다중 홉 경로의 중간 라우터에 사용할 수 없습니다. 이 오버레이 방법은 트래픽 변동성을 허용하지 않으며, ECMP(Equal Cost Multi-Path) 및 LAG(Link Aggregation Group) 경로를 차단합니다. 또한 효율적으로 확장되지 않으며 지연 시간을 증가시킵니다. 대역폭 요구 사항이 증가하고 데이터 흐름이 점점 메시 구조로 되면서 암호화된 게이트웨이에 더 빠른 속도의 포트가 필요하여 비용이 급증합니다.

암호화된 VPN 게이트웨이 오버레이를 사용하여 클라우드 보안을 유지하는 방법의 주요 단점은 다음과 같습니다.

- 복잡한 네트워크 아키텍처, 설계 및 엔지니어링
- 데이터 센터 간 트래픽 운영 및 관리에 필요한 전문 기술
- 매우 비효율적인 확장성
- 데이터 센터 간의 지연 시간 증가
- 패킷 계층 암호화 기술로 인한 전체 패킷 처리량 감소
- 모니터링, 문제 해결 및 기타 운영 문제
- 고가의 암호화된 게이트웨이 장비

앞서 설명했듯이, 트래픽 흐름이 증가하면 암호화 게이트웨이에 더 빠른 속도의 포트가 필요합니다. 이러한 패킷 기반 아키텍처는 확장성이 나쁘며, 암호화 장치가 매우 커지고 많은 비용이 소요되고 데이터 센터 간의 암호화된 링크에서 전체 처리량을 제공하기 어렵습니다. 이 확장성 문제를 해결하고 보다 높은 트래픽 부하에서 전문화된 암호화 게이트웨이 장비 비용을 절감하기 위해 조직에서는 해당 트래픽의 프로파일링을 시도할 수 있습니다. 프로파일링한 후에는 필요에 따라 암호화되거나 암호화되지 않은 게이트웨이를 통해 암호화된 경로와 암호화되지 않은 경로 간에 트래픽을 분할할 수 있습니다(그림 3). 이렇게 하면 암호화가 필요한 트래픽은 암호화된 게이트웨이로 전송하고 다른 모든 트래픽은 암호화되지 않은 게이트웨이로 오프로드하여 암호화된 게이트웨이의 확장성 문제를 완화할 수 있습니다.

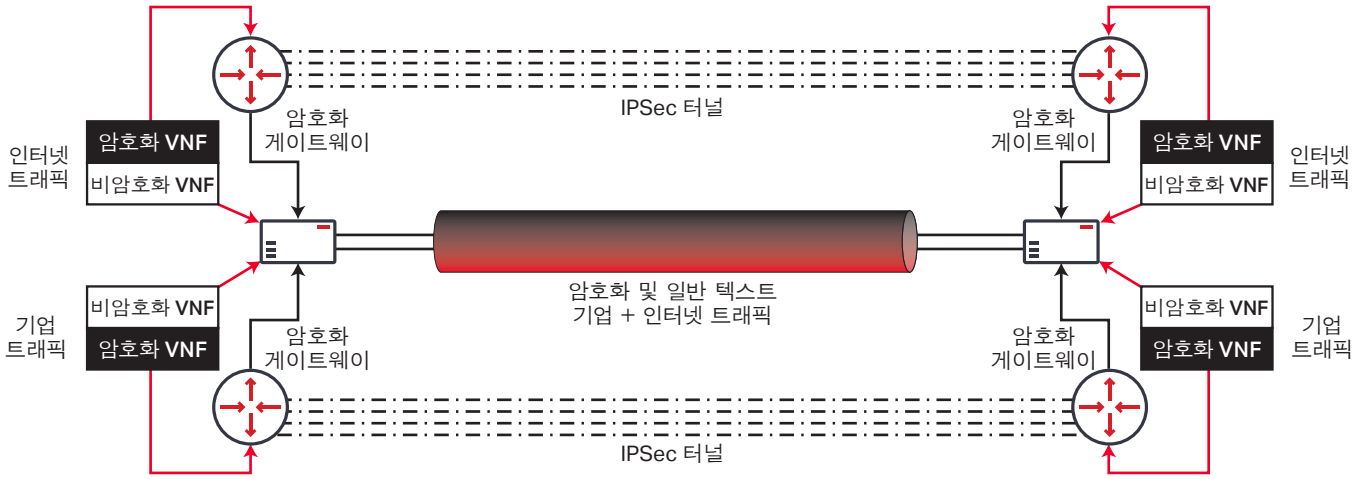

그림 3. 암호화 게이트웨이의 비용을 절감하기 위한 트래픽 프로파일링(논리 뷰)

그러나 트래픽 프로파일링과 관련하여 해결해야 하는 과제도 있습니다. 트래픽을 암호화해야 하는지 여부를 정확히 결정하기가 까다로울 수 있습니다. 이를 정확히 구분할 정도로 자체 데이터를 잘 알고 있는 조직은 거의 없으며, 트래픽을 잘못 식별할 경우 민감한 데이터가 보호되지 않은 상태로 방치될 수 있습니다. 애플리케이션 용도와 매개 변수가 자주 업데이트되므로 트래픽 프로파일이 이러한 변경 사항과 동기화된 상태로 유지되지 않으면 민감한 데이터가 보호되지 않은 경로를 통해 전송될 수 있습니다.

암호화된 게이트웨이 및 암호화되지 않은 게이트웨이와 함께 트래픽 프로파일링을 사용하는 방법의 주요 단점은 다음과 같습니다.

- 복잡한 네트워크 아키텍처, 설계 및 엔지니어링
- 데이터 센터 간 트래픽 운영 및 관리에 필요한 전문 기술
- 트래픽을 암호화된 것과 암호화되지 않은 것으로 프로파일링하는 작업의 높은 오류율
- 애플리케이션 용도는 시간이 지남에 따라 변경되므로 애플리케이션 프로파일과 트래픽 프로파일이 일치하고 동기화되어야 함
- 네트워크 하드웨어에서 일반/비암호화 라우팅 인스턴스와 암호화 라우팅 인스턴스를 설계 및 구현하기 복잡함
- 데이터 센터 간의 지연 시간 증가
- 패킷 계층 암호화 기술로 인한 전체 패킷 처리량 감소
- 고가의 암호화된 게이트웨이 장비

이러한 속성의 트래픽 프로파일링을 글로벌 수준으로 확장하는 것은 매우 까다로우며 시간이 지날수록 유지 관리하기 어렵습니다. 트래픽 보안을 적절히 유지하기 위해서는 신규 및 기존 애플리케이션과 데이터 소스에 대한 트래픽 프로파일을 지속적으로 업데이트해야 합니다. 트래픽 프로파일링이 성공하려면 애플리케이션 개발자, 보안 엔지니어, 시스템 및 네트워크 관리자 간에 일관되고 밀접한 통합이 보장되어야 합니다.

두 가지 패킷 계층 암호화 방법 모두 확장성 및 구현 복잡성 면에서 단점이 있습니다. 하지만 다행히 광 계층에서 전송 중 트래픽을 암호화하여 복잡성을 줄이고 확장성을 개선할 수 있는 새로운 옵션이 존재합니다.

24/7 데이터 보안 솔루션

광 계층 암호화: 간단한 보안 접근법

민감한 데이터만 보호하기 위해 리소스를 프로파일링하고 트래픽을 분리하는 데 시간을 허비하는 대신 모든 데이터를 보호하면서 구현하기 쉬운 광 계층을 암호화 솔루션으로 선호하는 조직이 증가하고 있습니다. Layer 1 또는 광 계층 암호화는 전체 OTN 페이로드를 암호화하여 상위 계층 통신으로부터의 모든 메시징, 헤더 및 데이터 보안을 유지합니다 (그림 4).

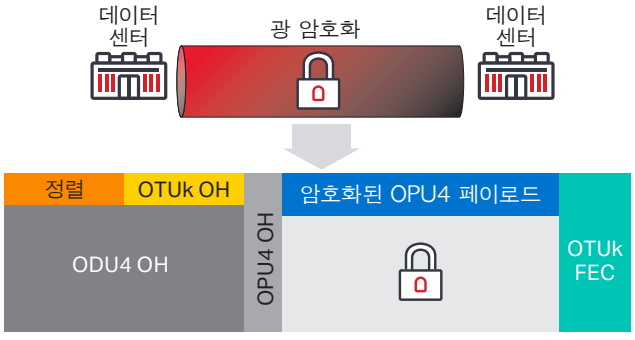

그림 4. Layer 1 암호화로 모든 트래픽 보안 유지

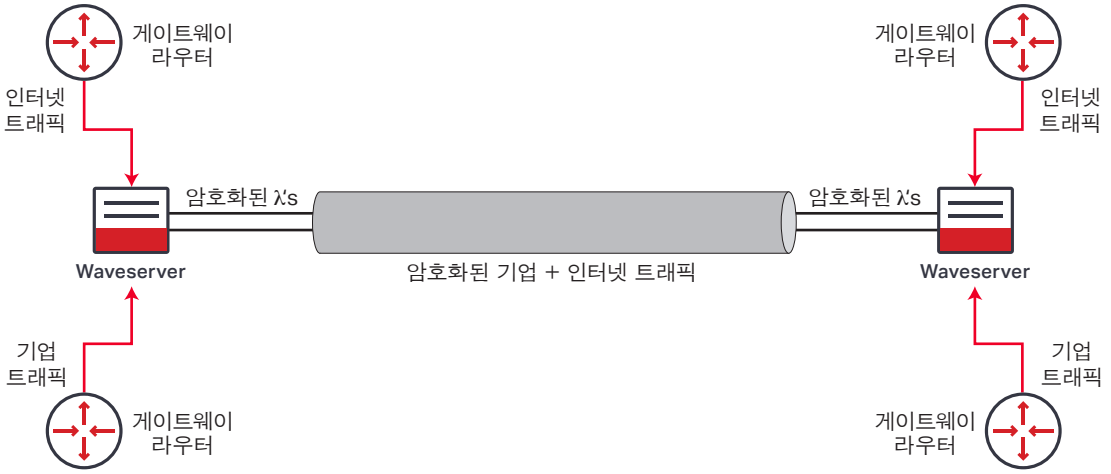

그림 5. 광 계층에서 모든 트래픽 보안 유지(논리 뷰)

광 계층 암호화는 네트워크 아키텍처를 간소화합니다(그림 5). 게이트웨이 라우터가 대용량 암호화를 위해 트래픽을 전송 장치(이 예의 경우 Waveserver®)로 직접 전송합니다. 고가의 암호화 게이트웨이가 필요하지 않으며, 암호화해야 하는 트래픽을 식별하기 위한 트래픽 프로파일링도 필요 없습니다. 데이터 센터에서 나가는 모든 트래픽은 회선 속도에서 전체 처리량으로 암호화됩니다.

Layer 1 암호화는 다음과 같은 장점을 제공합니다.

- **트래픽을 암호화하기 위한 추가 VPN 요구 사항이 없음** - Layer 1 암호화는 모든 트래픽을 암호화할 수 있는 솔루션을 제공하므로 암호화되거나 암호화되지 않은 VPN으로 전송하기 위해 트래픽을 프로파일링할 필요가 없습니다. 모든 통신의 보안이 유지됩니다.
- **무시해도 될 정도의 지연 시간** - Layer 1에서 암호화를 수행하면 나노초 내지 마이크로초의 지연 시간이 추가되는 반면, IPsec 또는 애플리케이션 계층 암호화와 같은 상위 계층 솔루션은 수백 밀리초의 지연 시간이 추가될 수 있습니다.
- **전체 처리량** - 전송 계층 페이로드만 암호화되므로 라우터 및 스위치의 패킷 계층 처리량이 영향을 받지 않습니다. Layer 1 회선 속도 암호화 솔루션은 트래픽이 암호화된 경우 전체 속도 처리량을 제공합니다.
- **구축, 설계 및 운영 간소성** - Layer 1 암호화 솔루션은 메트로 또는 장거리 네트워크 전반에 걸쳐 DWDM(고밀도 파장 분할 다중 방식) 전송을 제공하는 데 사용되는 것과 동일한 광 전송 시스템에 내장되므로 추가 암호화 어플라이언스가 필요하지 않습니다.
- **다중 프로토콜 지원** - Layer 1은 이더넷, IP, SONET/SDH, Fibre Channel 등 여러 유형의 트래픽을 지원하므로 필요한 암호화 어플라이언스 수가 감소하며, 단일 프로토콜(IP)로 제한된 IPSec과 같은 옵션에 비해 프로토콜 지원이 증가합니다.

Layer 1 암호화로 전환하면 클라우드 보안을 유지할 수 있는 간단한 솔루션이 제공됩니다. 보호된 링크를 통해 전달되는 모든 전송 중 데이터에 대한 대용량 암호화가 지원됩니다. Layer 1 암호화의 또 다른 장점은 최하위 계층에서 포괄적으로 사용될 수 있다는 점입니다. 보안 조직은 규정을 준수하기 위해 또는 필요한 경우 보다 포괄적인 보안 계획의 일환으로 여전히 상위 계층 암호화 솔루션을 개발하고 엔지니어링할 수 있지만 상위 계층이 노출된 경우에도 데이터는 계속 광 계층에서 암호화됩니다. 조직에서는 글로벌 보안 정책을 개발 중인 위치에 따라 포괄적인 보안 계획을 엔지니어링하거나 Layer 1 암호화를 포괄적으로 적용할 수 있습니다.

Ciena의 WaveLogic Encryption 솔루션

Ciena는 보안이 적용되지 않는 노출된 링크를 통해 데이터를 전달하는 대신 AES-256 암호화 알고리즘으로 데이터의 보안을 유지할 수 있는 Layer 1 암호화를 제공합니다. 또한 공격자가 물리적 매체에 대한 접근 권한을 얻고 광 케이블에 침투하려는 경우 모든 데이터가 암호화되고 사용할 수 없게 됩니다.

Ciena의 WaveLogic Encryption은 광 전송 네트워킹 장비에 통합된 구현하기 쉬운 회선 속도 광 암호화 솔루션을 제공합니다. 설치 후 사후 관리가 필요 없는 접근법을 통해 암호화가 항상 적용되므로 모든 데이터가 전송 중에 늘 보호됩니다. 따라서 민감한 데이터가 암호화되지 않은 상태로 네트워크를 통해 전송될 수 있는 실수가 제거됩니다.

Ciena의 솔루션은 ECC(Elliptic Curve Cryptography)를 비롯한 최신 공개 키 암호화 알고리즘을 지원하는 FIPS 인증 AES-256 암호화 엔진을 제공합니다. WaveLogic Encryption은 Ciena의 6500 Packet-Optical Platform과 Waveserver Stackable Interconnect 플랫폼 제품군에서 사용할 수 있으며, 100G QPSK, 150G 8QAM, 200G 16QAM, 단일 반송파 400G 등 다양한 회선 속도에서 회선 속도 암호화를 제공하도록 프로그래밍할 수 있는 코히어런트 WDM 인터페이스를 활용합니다.

Ciena의 6500을 사용하는 경우 사업자는 10G 암호화에 일체형 먹스폰더 기반 카드 솔루션을 활용하거나, 100G/200G 회선 모듈을 클라이언트 인터페이스 카드와 함께 쌍으로 활용하여 특정 트래픽 요구 사항을 유연하게 충족할 수 있습니다. 또한 Waveserver를 활용하여 1RU에서 최대 400G 용량의 AES-256 회선 속도 암호화 기능을 구축하고 뛰어난 유연성을 통해 동일한 장치에서 10GE, 40GE 및 100GE 클라이언트 혼합을 지원할 수 있습니다. 100GE 클라이언트 인터페이스에 최적화된 Waveserver Ai를 사용하면 단일 랙 유닛에 최대 1.2T 용량의 암호화 기능을 구축할 수 있습니다.

Ciena의 코히어런트 전송에 내장된 회선 측 프로그램 기능을 통해 사업자는 모든 애플리케이션 요구 사항에 맞게 회선 용량을 최적화하고 메트로, 외곽 또는 장거리에 걸쳐 전송 중 데이터의 보안을 유지할 수 있습니다. 따라서 사용 중인 기본 포토닉 회선 시스템 또는 거리에 상관없이 데이터 센터 간의 연결성 보안이 유지됩니다.

6500과 Waveserver를 둘 다 구축하면 상위 수준 애플리케이션 또는 IP 기반 인프라 솔루션과 연관된 복잡성 없이 클라우드의 보안을 유지할 수 있습니다. 점점 더 민감한 정보가 광 케이블 네트워크를 통해 분산되고 법률과 규정에서 데이터 보안에 대한 요구가 강화되는 상황에서 오늘날의 클라우드 기반 통신은 서버 보안과 저장 중 암호화뿐만 아니라 강력한 전송 중 암호화 솔루션까지도 포괄하는 IT 보안 접근법을 구축해야 합니다.

간편한 암호화 솔루션 자세히 알아보기

결론

포괄적인 보안 계획을 수립하는 것은 특히 데이터 센터 간의 애플리케이션 간 통신을 고려할 때 까다로운 일일 수 있습니다. 조직에서는 데이터 센터 간에 전달되는 데이터의 보안을 유지할 수 있는 방안을 마련하기 위해 네트워크 인프라에 의존하는 경우가 많습니다. 그러나 Layer 3에서 네트워크 암호화를 제공하는 것은 비용이 많이 들고 확장하기 어려울 수 있습니다. 다행히 광 계층 암호화는 첫 번째 수준에서의 방어를 제공하며 간단하게 구현할 수 있습니다. 프로토콜 제약이 없으므로 다양한 트래픽 유형을 지원할 수 있습니다. 과도한 부하에서 처리량 감소 없이 회선 속도 암호화를 제공하며, 추가 지연 시간이 거의 없습니다. Layer 1 암호화는 데이터 센터 간에 전달될 때 전송 중 데이터를 보호하는 비용 효과적인 방법을 제공하며, Ciena의 WaveLogic Encryption 솔루션은 뛰어난 유연성 및 보안성을 운영 및 관리 용이성과 결합한 솔루션입니다. 이와 함께 거리, 도시, 국가 또는 해양 전반에서 항상 데이터 센터 간 통신의 보안을 유지하는 비용 효과적인 대용량 회선 속도 암호화를 구현합니다.

Ciena 커뮤니티를 방문하여 질문에 대한 답변을 받아보세요