애플리케이션 정보

WaveLogic Encryption 솔루션

모든 전송 중 데이터에 대한 상시 보호

보안은 이제 모든 조직이 직면한 현안이 되었습니다. 2020 Thales Data Threat Report[1]에 따르면 조사에 참여한 글로벌 기업의 49%가 기업 역사의 어떤 시점에 데이터 유출로 피해를 입은 적이 있다고 답했습니다. 특히 데이터 유출로 인해 의료, 금융, 정부 및 교육과 같은 산업 부문은 평균보다 훨씬 많은 손실을 기록했습니다.

보안 문제가 발생하면 고객 정보가 위험해질 뿐 아니라 조직의 재정에도 영향이 갑니다. Ponemon의 글로벌 연구[2]에 따르면 데이터 유출이 발생할 때마다 약 25,500개의 기록이 노출되며, 데이터 유출 한건당 수 백만 달러의 비용 손실이 발생하고 고객 신뢰 하락으로 인한 손실은 측정할 수도 없습니다. 또한 이 연구에서는 2019년 미국에서 데이터 유출로 인한 평균 비용이 819만 달러에 달한다고 밝히고 있습니다. 다시 말하자면 이러한 피해는 산업별로 다양하며 의료 산업의 경우 기록 손실당 비용은 거의 2배에 이릅니다.

데이터 유출 위협이 증가하는 상황에서도 네트워크를 통해 전송되는 트래픽 양은 증가하고 있습니다. 대역폭 수요가 지속적으로 증가함에 따라 운영 복잡성 없이 용량 증가를 처리할 수 있도록 네트워크를 단계적으로 확장할 수 있어야 합니다. 또한 데이터 유출 수단이 정교해지고 그 빈도가 증가함에 따라 중요 정보와 개인 정보를 수집하려는 악의적 공격의 영향을 받지 않는 조직은 더 이상 존재하지 않습니다. 오늘날의 고용량 네트워크는 훨씬 많은 대역폭 용량을 필요로 하며 메트로, 지역 및 장거리 분야로 그 운용 범위를 확대하고 있기 때문에 저장 중 데이터와 전송 중 데이터 모두를 보호할 수 있는 보안 전략이 필요합니다.

이러한 고용량 네트워크를 보호하도록 설계된 Ciena의 WaveLogic Encryption™은 프로토콜 제약이 없고 지연 시간이 매우 낮은 확장형 솔루션으로, 전 세계 현장에서 운용되고 있는 6500 Packet-Optical Platform을 기반으로 합니다. 이 솔루션은 Ciena Waveserver® 제품군의 소형 고용량 모듈식 전송 장치로도 확장되어 비용 효과적이고 안전한 DCI(데이터 센터 상호 연결) 애플리케이션을 지원합니다. 상시 가동되는 이 암호화 솔루션은 쉬운 운영과 관리를 특징으로 하며, 산업을 선도하는 Ciena의 WaveLogic 코히어런트 기술을 활용하는 데이터 보호 전략을 편리하게 이행하도록 지원함으로써 전례 없는 수준의 유연성과 성능을 보유한 업계 최초의 코히어런트 100G ~ 400G 회선 속도 암호화 기능을 전달합니다.

이점

- 높은 수준의 보안성과 투명성을 가진 종단 간 통신을 위해 초저 지연 시간의 FIPS 인증 암호화 솔루션을 제공합니다.
- 유연한 100G ~ 400G 회선 속도 암호화를 지원하는 프로그래밍 가능한 WaveLogic 3 코히어런트 기술을 통해 확장합니다.
- 프로토콜 제약이 없는 암호화 기술을 특징으로 하며 탁월한 유연성으로 다양한 서비스를 지원합니다.
- 인증 기능과 데이터 암호화 기능을 위한 2종의 개별 키 세트 (초 단위로 빠르게 암호화 키 교대)를 비롯한 첨단 보안 기능을 활용합니다.
- X.509 인증서 기반 인증을 사용하여 기존의 기업 PKI(Public Key Infrastructure)에 매끄럽게 통합됩니다.
- 통합된 관리 도구를 통해 최종 사용자가 EaaS(Encryption-as-a-Service) 기능을 안전하게 관리할 수 있습니다.
- 전 세계에서 운용 중인 금융, 법률, 의료, 군사, 전력 기관 및 정부 기관 네트워크에서 널리 활용되고 현장에서 입증된 암호화 솔루션을 제공합니다.

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Ponemon, IBM 연구: Cost of a Data Breach 2020: https://www.ibm.com/security/data-breach

암호화 기술

암호화는 암호화 키라고 하는 특별한 처리 기술을 사용하지 않고는 판독할 수 없는 알고리즘을 통해 정보를 변환하는 프로세스로 정의됩니다. 기본적으로 이 프로세스는 데이터를 검색한 무단 침입자나 적합한 메시지 판독용 키를 보유하지 않은 사용자가 사용할 수 없도록 데이터를 변환하는 방식으로 데이터를 암호화함으로써 네트워크를 봉쇄합니다.

제품과 키 지원에 대한 암호화 요구와 네트워크 장비에 대한 인증 프로세스 세트에 대한 암호화 요구를 규정한 여러 표준이 있으며 이러한 표준에서 정의한 다양한 데이터 암호화 방법이 존재합니다. NIST(미국 표준 기술원)에서 공개한 다양한 키 크기(56비트, 128비트, 256비트)를 가진 AES(Advanced Encryption Standard)와 같은 표준 기반 암호화 알고리즘도 있습니다. 이러한 표준들은 FIPS(미국 연방 정보 처리 표준) 발행물 형태로 공개됩니다. 예를 들어 AES-256 암호화 알고리즘은 FIPS 197로 발표되었습니다. FIPS 197과 같은 알고리즘 관련 발행물 이외에도 NIST는 FIPS 140-2의 하드웨어와 소프트웨어 구성 요소를 모두 포함하는 암호화 모듈에 대한 요구 사항을 명시하는 표준도 공개합니다.

암호화 솔루션 인증을 위해 사용되는 다른 비슷한 프레임워크도 있습니다. 다른 중요한 표준으로는 정보 기술 보안 평가를 위한 CC(공통 평가 기준)가 있으며 이는 컴퓨터 보안 인증을 위한 국제 표준(ISO/IEC 15408)입니다. CC는 광 네트워크의 네트워크 요소와 같은 네트워크 장치의 사양, 구현 및 평가와 관련된 프로세스가 엄격한 표준 방식을 준수하도록 보장하는 수단을 제공합니다. 독일의 BSI(연방 정보 보안청)는 CC에 대한 인증을 포함하는 보안 인증서를 발급합니다. CC에 기반하는 BSI 인증서는 주로 로컬 인증의 토대로 사용되므로 인증 프로세스에서 시간과 비용이 단축됩니다. 이러한 표준 및 인증 프로세스 집합을 통해 서비스 공급자와 최종 사용자는 표준에서 의무적으로 요구하는 엄격한 연구소 테스트와 검토 과정을 성공적으로 수행함으로써 암호화 솔루션이 표준에서 명시한 요구 사항을 준수할 수 있도록 보장할 수 있습니다.

그림 1. 종합적인 보안 전략의 일부분인 전송 중 데이터 암호화

네트워크 보안 강화

오늘날 암호화는 저장 중 데이터와 전송 중 데이터 모두를 보호하기 위해 널리 사용되는 기술입니다. 암호화 추세를 연구한 Ponemon 보고서에 따르면 조사에 참여한 전 세계 응답자 중 13%만이 암호화 전략이 없다고 대답했습니다.[3] 소속된 산업에 상관 없이 모든 규모의 조직들은 데이터 센터에 저장된 정보를 무단 접근으로부터 보호하기 위해 모든 노력을 기울여야 합니다. 데이터 유출로 인한 영향과 손실 비용은 무시할 수 없는 수준이며, 기업 평판 악화, 형사 고소, 규제 위반 벌금 그리고 가입자 이탈을 포함하여 지속적으로 심각한 결과를 초래하고 있습니다.

오늘날 널리 사용되는 기술들은 사용자 접근과 자격 증명을 관리함으로써 서버, 데이터베이스, 라우터 및 스위치에 대한 무단 침입을 방지하여 저장 중인 데이터를 보호합니다. 그러나 데이터는 데이터 센터 경계 너머에서 고대역폭 통신을 통해 전 세계를 아우르는 거대 네트워크를 통과하기 때문에 오늘날의 웹스케일 네트워크에서 엄청난 양의 중요 데이터가 전송 중인 상태로 있습니다. 따라서 종합적인 IT 보안 접근법은 전체 보안 전략의 일부로 견고한 전송 중 암호화 솔루션을 통합하고 있어야 합니다(그림 1 참조). 사설 클라우드 보안 기능처럼 데이터를 암호화하는 사업자는 데이터가 네트워크에서 전송될 때 다양한 보안 계층을 통과하여 목적지에 도달하는 순간까지 무단 데이터 탈취로부터 데이터를 보호할 수 있습니다.

많은 조직들이 전송 중 데이터 암호화 기능을 보안 전략에 포함시키고 있는 상황에서, 전통적인 보안 기능이 Layer 2 이상에서 전송 중 데이터를 암호화하기 위해 사용되고 있습니다. 그러나 데이터 집중도가 높지 않거나 시간이 중요하지 않은 저속 IT 애플리케이션에서 이 방식은 좋은 선택일 수 있지만 전사적 범위에서는 효율적이지 않고 IP 애플리케이션 데이터만을 암호화하는 단점이 있습니다. 암호화 측면에서 이 모델은 운영하기가 까다롭고 비용이 많이 듭니다(그림 2 참조). 프로토콜에 특정한 독립 실행형 암호화 장치를 필요로 하고 상당한 지연 시간을 발생시켜 애플리케이션 처리량에 악영향을

3 Ponemon, Thales e-Security 연구 보고서: 2018 Global Encryption Trends Study, 2018년 4월.
https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

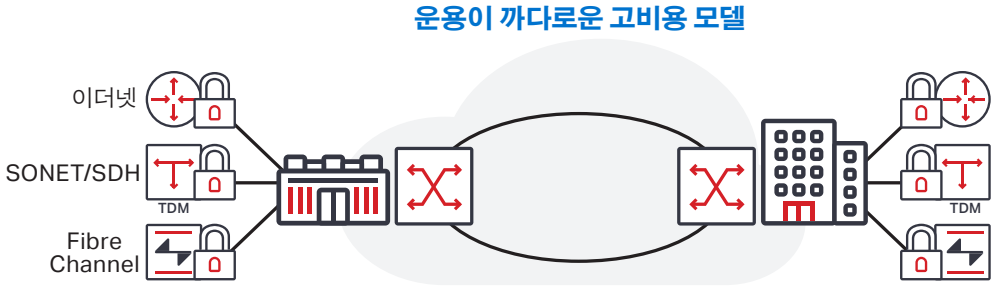

그림 2. 다중 서비스 네트워크에서 운용되는 전통적인 프로토콜 특정 암호화

주고 비효율적인 대역폭 사용을 초래하기 때문입니다. 또한 독립된 다양한 장치 간에 암호화 키 관리와 인증이 복잡하고 많은 노동력을 필요로 하며, 종단 간에 걸쳐 네트워크에서 문제를 해결하려면 많은 독립 장치에서 매우 복잡한 작업이 수반됩니다. 뿐만 아니라 이 접근법은 조직의 전송 중 데이터 암호화 전략에 빈틈을 만듭니다. 전통적으로 광 케이블 침입에 대한 위험성은 조직의 보안 전략에서 고려되지 않지만, 광 케이블로 전송되는 데이터에 액세스하기 위해 광 케이블에 침입하는 것이 실제적이 위협이 되고 있습니다. 일반적으로 광 케이블에는 보호 수단이 없어 쉽게 접근할 수 있으며 누구라도 적합한 도구만 있으면 광 케이블을 도청하여 보호되지 않은 데이터를 여러 날, 여러 달, 심지어는 여러 해 동안 수집할 수 있습니다. 전송 계층 암호화 솔루션을 운용하면 모든 전송 중 데이터를 상시로 보호하여 모든 트래픽의 안전을 보장할 수 있습니다.

Data Security with Optical Encryption 인포그래픽 지금 다운로드

WaveLogic Encryption

네트워크 데이터의 기밀성, 무결성 및 가성용을 보장하는 Ciena 다중 계층 보안 접근법의 일부인 Ciena WaveLogic Encryption은 대규모 글로벌 설치 기반을 가진 플랫폼에 구축된 입증된 암호화 기술을 전 세계 600여 개 이상의 사업자가 구축한 6500 Packet-Optical Platform의 입증된 안정성과 결합한 솔루션입니다. 또한 Ciena의 WaveLogic Encryption 기능을 Ciena의 Waveserver 및 Waveserver Ai 장비까지 확대 운용하여 1RU에서 최대 1.2Tb 회선 속도 암호화 솔루션을 제공할 수 있으며 그 결과 간소화된 랙 적층형 DCI 애플리케이션을 구현할 수 있습니다.

간편한 운용

WaveLogic Encryption 암호화 솔루션을 도입한 사업자는 암호화 기능을 전송 네트워크 내의 네트워크 요소에 직접 통합함으로써 암호화 기능 운용을 간소화할 수 있는 이점을 얻을 수 있습니다. 이 접근법을 활용하면 네트워크 복잡성이 해소되고 다양한 애플리케이션에서 서로 다른 암호화 솔루션을 관리할 필요가 없습니다(그림 3 참조). 운영 측면의 이러한 간소성은 관리 측면으로 확대됩니다. 즉 전용 인증 및 키 관리 도구를 편리하게 관리하고 기존 기업 PKI에 쉽게 통합할 수 있습니다.

6500 플랫폼의 뛰어난 유연성을 통해 고객은 사이트별로 다양한 용량, 공간 및 전력 요구에 적합한 최적 크기의 셀프를 선택함으로써 암호화 서비스를 비용 효과적으로 전달할 수 있습니다. 다른 중요한 이점은 프로토콜 제약이 전혀 없기 때문에 이더넷, SONET/SDH, Fibre Channel 및 OTN을 포함하여 매우 다양한 클라이언트를 유연하게 지원함으로써 보안을 중요하게 고려하는 고객을 위해 다양한 애플리케이션 요구를 충족시킬 수 있습니다.

상시 가동되는 암호화 기능으로 차별화 달성

암호화 기능이 Ciena의 WaveLogic Encryption 솔루션에서 상시로 가동되어 모든 네트워크 트래픽을 항상 암호화하기

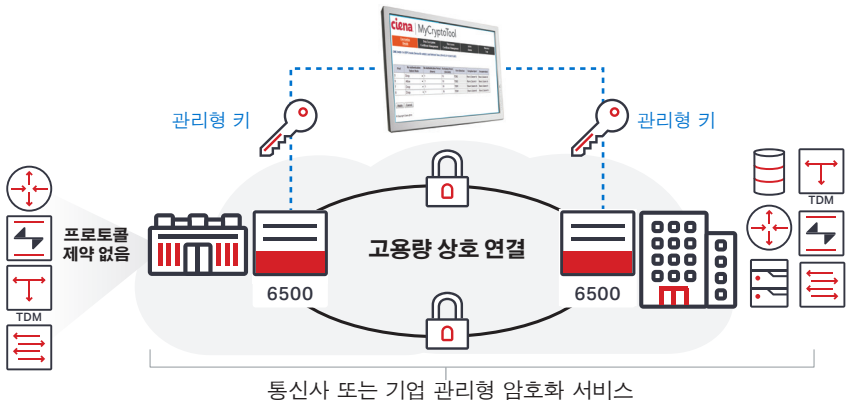

그림 3. Ciena의 6500 WaveLogic Encryption 솔루션

때문에 가장 높은 수준의 보안성을 확보할 수 있습니다. 상황에 따라 암호화 기능을 켜거나 끄는 것이 유연하게 보일 수는 있지만 사람이 만드는 작은 오류로 인해 중요한 트래픽을 암호화되지 않은 네트워크로 보내버릴 수 있습니다. 사업자는 전 세계의 메트로, 지역, 장거리 또는 해저 범위를 아우르는 차별화된 인프라를 활용하여 모든 전송 중 데이터를 상시 보호할 수 있습니다. 또한 초저 지연 시간 연결과 다양한 경로/장비 보호 옵션을 가진 암호화 서비스를 활용하여 차별화된 고속 SLA(서비스 수준 계약)를 제공함으로써 수익을 증가시키고 더 많은 고객을 유치할 수 있습니다.

가장 견고한 암호화 기능

Ciena의 WaveLogic Encryption 솔루션은 외부에서 검증하고 제3자가 수행하는 독립적 인증 절차를 거치기 때문에 CC(공통 평가 기준) 및 FIPS 인증을 포함한 산업 표준 알고리즘과 첨단 보안 기능을 활용하여 이 솔루션을 효과적으로 구현할 수 있습니다. 즉 X.509 인증과 같은 표준 기반 인증 체계와 함께 FIPS 인증 AES-256 암호화 엔진을 제공하여 기존 기업 PKI에 매끄럽게 통합할 수 있습니다. 또한 암호화 모듈의 6500 하드웨어와 소프트웨어 구성 요소가 FIPS 140-2 표준과 정보 기술 보안 평가를 위한 CC 표준에 따라 완전한 BSI 인증을 준수하기 때문에 서비스 공급자와 최종 사용자는 이 포괄적인 평가 표준에서 다루는 모든 요구(예: 암호화 알고리즘, 키 교환 체계 및 사용자 인증 등)를 준수하는 이 암호화 솔루션을 안심하고 운용할 수 있습니다.

더 높은 수준의 보안을 위해 별개의 독립적인 2종의 키가 인증 기능과 데이터 암호화 기능을 위해 사용됩니다. 이때 분 단위가 아닌 초 단위 간격으로 빠르게 암호화 키가 교환됩니다. AES-256 데이터 암호화 세션 키는 사용자의 간섭 없이 그리고 트래픽이나 처리량에 영향을 주지 않고 자체적으로 교섭되고 각 회선 포트에서 매 초마다 독립적으로 교환됩니다. 통신 사업자는 ECC(Elliptic Curve Cryptography)를 지원하는 차세대 공용 키 암호화 알고리즘을 활용할 수 있습니다. ECC는 1세대 공용 키 암호화 시스템보다 훨씬 뛰어난 보안화 전략을 제공합니다.

프로그래밍 가능한 100G ~ 400G 회선 속도 암호화

오늘날 고용량 통신에서 발생하는 요구를 충족시키기 위해 Ciena의 WaveLogic Encryption 솔루션은 산업을 선도하는 WaveLogic 코히어런트 기술을 활용하여 유연하고 맞춤 가능한 고용량 암호화 솔루션을 구현합니다. WaveLogic 3 Extreme은 WaveLogic 3의 기능을 기반으로 개발되었으며, 추가적인 변조 기술을 사용하고 선형 및 비선형 장애를 개선하는 기능을 통해 모든 코히어런트 네트워킹 애플리케이션에 최고의 성능을 제공합니다. 이 최첨단 솔루션은 소프트웨어로 프로그래밍할 수 있는 변조 기술을 제공하여 QPSK 변조를 사용하는 100G 회선 속도 암호화 기능, 8QAM 변조를 사용하는 150G 회선 속도 암호화 기능 그리고 16QAM 변조를 사용하는 200G 회선 속도 암호화 기능을 지원합니다. WaveLogic Ai는 업계 최고의 성능을 가진 WaveLogic 3 기술을 기반으로 개발되었으며 첨단 400G 최적 엔진을 사용하여 전송 경제성을 획기적으로 개선합니다. 즉 채널당 용량을 2배 증가시키고 동등 용량의 전송 거리를 3배 확대하며 서비스 밀도를 4배 강화합니다.

6500 플랫폼을 운용하는 통신 사업자는 이 WaveLogic 3 Extreme 회선 모듈을 다양한 클라어언트 인터페이스와 함께 암호화 기능과 통합함으로써 특정 트래픽 요구(10G, 40G 또는 100G 서비스 전송)를 효과적으로 충족시키는 맞춤형 솔루션을 유연하게 운용할 수 있습니다. 사용량에 따라 비용을 지불하는(pay-as-you-grow) 모듈 방식으로 트래픽 수요가 증가하는 경우 추가 클라이언트 카드를 연결하여 암호화된 200G 트래픽을 전송하도록 동일한 회선 모듈을 프로그래밍할 수 있습니다. 뿐만 아니라 6500의 고용량 하이브리드 패킷/OTN 패브릭을 활용하여 고용량 암호화 서비스를 네트워크 전반에서 운용할 수 있어 네트워크 리소스 효율성을 극대화할 수 있습니다.

Waveserver를 운용하는 사업자는 1RU에서 최대 400Gb/s 용량의 FIPS 인증 AES-256 회선 속도 암호화 기능을 활용하고 뛰어난 유연성을 통해 동일한 장비에서 10GE, 40GE 및 100GE 클라이언트 혼합을 지원할 수 있습니다. 프로그래밍 가능 변조 기술을 사용하는 Waveserver는 2개의 100Gb/s, 150Gb/s 파장 또는 200Gb/s 파장을 제공하여 각 애플리케이션/요구에 따라 회선 속도 암호화 용량을 최적화할 수 있습니다. 초고용량 보안 상호 연결 애플리케이션 요구를 해결하기 위해 사업자는 Waveserver Ai를 운용하여 1RU에서 최대 1.2Tb/s 암호화 용량을 제공할 수 있으며 이와 함께 최대 400Gb/s 암호화 용량을 각각 제공하는 3개의 트래픽 모듈을 지원할 수 있습니다. Waveserver와 Waveserver Ai는 메트로, 지역 및 장거리 분야에서 높은 보안성과 초저 지연 시간 특성을 가진 전송 중 데이터 보호 기능을 제공합니다.

6500 10G 회선 속도 암호화

사업자는 암호화 모듈을 탑재한 4x10G Optical Transponder를 활용하여 10G 암호화 서비스를 비용 효과적으로 제공할 수 있습니다. 이 단일 슬롯 모듈은 프로토콜에 독립적인 10G 암호화 회선 포트 4개를 통해 40G의 회선 속도 암호화 서비스 용량을 제공합니다. 따라서 고객은 모든 6500 새시 변형 제품에서 통합된 암호화 기능을 통해 네트워크 설계를 간소화하는 이점을 얻을 수 있습니다. 또한 이 모듈은 FIPS 140-2 Level 3 호환 설계를 채택하여 강력한 보안성을 제공하며 초기화를 통해 카드에 대한 물리적 탬퍼링을 방지합니다. 즉, 암호화 모듈의 물리적 탬퍼링이 감지되면 카드가 셸프에 연결되지 않은 경우에도 모든 데이터를 영(0)으로 설정함으로써 중요한 모든 보안 정보를 삭제합니다.

High-capacity Wire-speed Encryption Modules 데이터시트 지금 다운로드

간소화된 암호화 관리

업계 최고의 전송 계층 보안 솔루션이라면 간소화된 통합 암호화 관리 접근법이 완비되어 있어야 합니다. 전송 관리에서 암호화 관리를 분리하면 사업자나 기업이 관리하는 인프라의 유연성이 더욱 향상됩니다. 어느 경우든, 데이터의 "소유자", 즉 최종 사용자가 종단 간에 걸쳐 보안 경보와 로그를 모니터링하는 동시에 보안 정책에서 요구하는 새로운 키나 인증서를 발급하는 방식으로 중요 데이터와 연관되는 암호화 보안 매개 변수에 대한 완전한 제어권을 보유하는 것이 중요합니다.

Ciena의 6500 WaveLogic Encryption 솔루션은 분산 네트워크 관리를 위해 설계된 전용 암호화 관리 인터페이스인 MyCryptoTool을 통합하고 있습니다. 이 도구를 사용하는 최종 사용자와 보안 책임자는 통신사 관리형 서비스나 기업 관리형 서비스의 보안 매개 변수와 경보를 독립적으로 관리할 수 있습니다. MyCryptoTool은 사용이 편리한 인터페이스이며 암호화 모듈에 대한 보안 연결을 구성하고 상호 인증을 제공하여 인증된 보안 사용자로만 액세스를 제한합니다. 서비스 공급자로부터 암호화된 서비스를 구입한 경우 서비스 공급자는 다른 서비스처럼 링크, 프로비저닝, 관리 및 성능 모니터링을 관리하지만 암호화 매개 변수에 대한 제어권이나 가시성은 보유하지 않습니다. 기업이나 정부 기관 내의 다른 두 부서에서 암호화 솔루션은 운용하고 관리하는 경우에도 이 접근법을 활용할 수 있습니다.

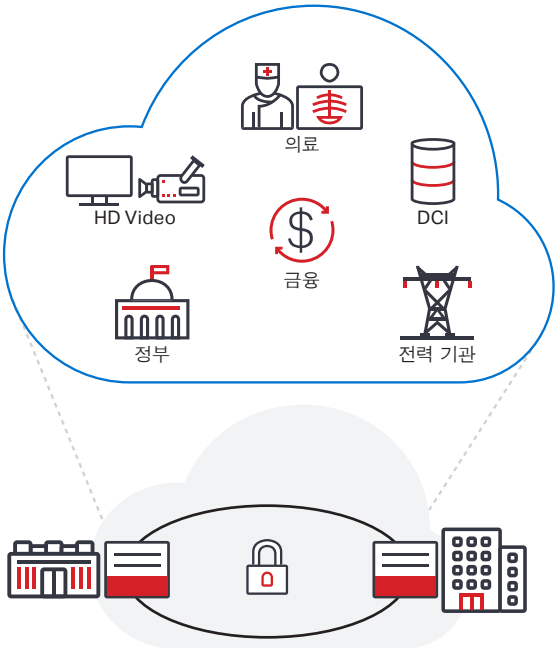

그림 4. WaveLogic Encryption 솔루션 운용 애플리케이션의 예

주요 애플리케이션

Ciena의 WaveLogic Encryption 솔루션은 오늘날의 모든 대용량 애플리케이션에서 전송 중인 중요 데이터를 보호하도록 맞춤형으로 설계되었습니다. 이러한 솔루션의 이점을 누릴 수 있는 주요 애플리케이션은 다음과 같습니다.

- 대용량 스토리지 및 데이터 암호화 전송을 위한 기업 DCI
- 다른 위치 간에 보안성이 뛰어나고 인증된 고속 통신을 필요로 하는 정부 기관
- 보안성, 효율성 및 적시성이 필요한 협업을 위해 낮은 지연 시간과 높은 품질 요구 사항을 충족시켜야 하는 의료 기관
- 관리형 서비스 애플리케이션
- 보안성이 뛰어난 초저 지연 시간 전송 솔루션을 필요로 하는 고해상도 영상 분야나 고속 금융 거래 분야와 같은 지연 시간이 중요한 애플리케이션
- 중요 통신 인프라를 보호하려는 전력 기관

요약

점점 더 많은 중요 정보가 광 케이블 네트워크를 통해 전송되는 상황에서 오늘날의 고용량 통신은 서버 보안과 저장 중 데이터 암호화 솔루션뿐 아니라 전송 중 데이터 암호화 솔루션까지도 포괄하는 IT 보안 접근법을 운용해야 합니다. Ciena의 WaveLogic Encryption은 가장 높은 수준의 유연성과 보안성을 쉬운 운영과 관리 특성에 결합함으로써 확장 가능하고 비용 효과적인 회선 속도 암호화 솔루션을 구현합니다. 그 결과 메트로, 지역, 장거리 또는 해저 분야를 비롯한 다양한 분야에서 모든 전송 중 데이터를 안전하게 상시 보호합니다.