ciena
Experience. Outcomes.

アプリケーションノート

クラウドをセキュアに

レイヤー1暗号化を使ってデータセンター間のセキュリティーを簡素化

機密データと極めて重要なデータの安全性を確保することは、知的財産や機密レコードをプロテクトし、データ漏洩による高額な罰金や利益の喪失を防ぐために必要不可欠な対策です。課題となるのは、プロテクトするデータと方法を判別することです。データセンターの物理設計では、物理的なセキュリティー対策を複数レイヤーで装備して不正アクセスを制限します。また、データセンター内のデータをプロテクトするために、ファイアウォール、ウイルス対策、侵入検知の手法を用いる場合があります。しかし、いったん情報がデータセンターの安全な領域から離れると、多くの場合、セキュリティーに対して注意が払われなくなります。

データセンターを相互接続するファイバー・ネットワークはセキュリティー攻撃の影響を受けないと考えられてきましたが、機密データがデータセンターとデバイス間や別のデータセンターのアプリケーションとの間でやり取りされる場合には、データセンター間の通信をなおざりにすることで脆弱性が生じます。データが組織の制御下にないリンクを通過する場合、漏洩や侵害のリスクにさらされることになります。

組織はデータセンター内のみならず、データセンター間でやり取りされるアプリケーションや情報の安全性を確保する必要があります。データセンター間のセキュリティーを設計、実装、スケーリングすることは難しいでしょうが、アプリケーション・レイヤーで暗号化することで、データセンター間の相互接続の安全性を確保できます。また、パケット・レイヤーの暗号化も役立ちますが、これらのタイプの暗号化にはいずれも独自の課題があります。3つ目に、最下位層であるネットワーキング・レイヤー、つまり光レイヤーでネットワーク・データを暗号化するというより魅力的な選択肢があります。光レイヤーの一括暗号化により、拡張性の高いアーキテクチャー、簡素化されたエンジニアリング、容易な運用が可能になり、データセンター間またはクラウド経由で伝送されるすべての転送中データがプロテクトされます。

必要不可欠なデータセンター間ネットワークのプロテクト

最近の調査により、約4分の1の組織が24カ月以内に大規模なデータ漏洩を経験する可能性があることが判明しました。[1] 被害者の特定および通知、関連法規の違反による罰金の支払いが必要になるため、漏洩にかかるコストは数百万ドルに及ぶ可能性があります。

レイヤー1暗号化のメリット：

- トラフィックの輻湊がない高速なスループット
- 安全性の高いデータセンター間通信を実現する超低遅延のワイヤースピード暗号化
- 追加の暗号化アプライアンスが不要の導入と運用が容易なソリューション
- さまざまなサービスに対応するプロトコルに依存しない柔軟な暗号化

1 Ponemon Institute「2017 Cost of Data Breach Study」、Ponemon Institute Research Report（2017年6月）、1-2

また、一度データ漏洩が起こると、収益の損失、顧客の喪失、評判の低下により、さらに多くのコストが発生する可能性があります。

規制により、セキュリティー侵害の識別および通知の義務づけがますます厳しくなっています。伝送されるデータまたはレコードのタイプに応じて、データの暗号化が義務づけられる場合があります。機密データが漏洩した場合には、企業に多額の罰金が課せられることがあり、収益全体に影響する可能性があります。

セキュリティーに関する新しい考え方

セキュリティーを検討するとき、組織は、セキュリティー侵害は起こり得るものであり、いずれは必ず起こるという新しい考え方を取り入れる必要があるでしょう。防御によって攻撃者がネットワークに侵入できなくなると想定することは推奨されません。代わりに、攻撃者がすでにネットワーク内に侵入している、または近い将来に侵入することを想定する必要があるかもしれません。セキュリティー侵害を想定した考え方を採用することで、データが常時プロテクトされるように防御を設計でき、侵入不可能なシステムの設計を試みたり、システム侵害後にデータのプロテクションを懸念したりする必要がなくなります。例えば、ネットワーク全体で転送中データを暗号化できるなら、たとえ攻撃者が転送中データをキャプチャーできたとしても、データを読み取ることができません。

キーとなるいくつかの条件が同時に成立していなければ、攻撃は成功しません。システムにソフトウェア・パッチが適用されていないなどの何らかの脆弱性があり、システムが攻撃者にとって価値のあるものであり、また、システムにアクセス可能であるという条件が満たされた場合、攻撃者が適切なツールと手法を備えていれば、セキュリティー侵害が起こる可能性があります。

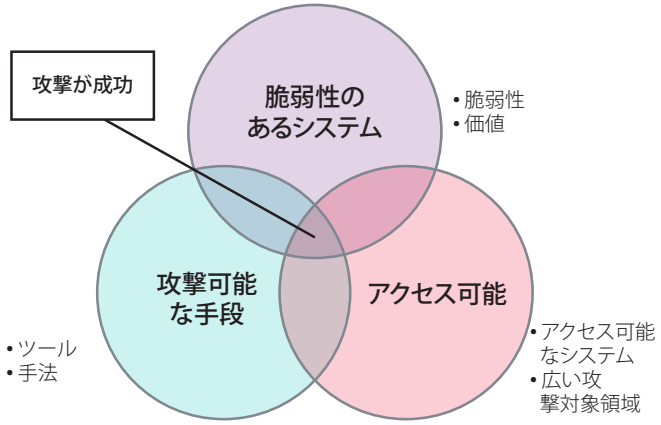

図1. 攻撃を成功させる条件

防御戦略を立てるには、資産の識別、アクセスの決定、脅威の理解という3つのステップを実行する必要があります。資産を識別するときには、組織はどれが重要な資産（データや機密レコード）であるか、また、その資産をどのようにプロテクトしてアクセスするかを理解していなければなりません。データベース内のデータは、データベースに適用されているプロテクションによって安全性が確保されますが、データベースからエクスポートされてネットワーク内を移動しているときには、データの状態はセキュアではなくなります。例えば、人事部がレポート作成用のデータをExcelにエクスポートした場合、データセンター間を転送されるスプレッドシートは暗号化されていないのでセキュアではありません。

包括的なセキュリティー戦略のためのネットワーク暗号化の追加

包括的なセキュリティー戦略の一環として、クラウドも含め、データセンター間を伝送されるすべてのデータをプロテクトすることは、かつてないほど重要になっています。ネットワークのいかなる部分もハッキングが不可能であると想定すべきではなく、転送中のデータをなおざりにすることは推奨されません。企業はデータの機密性を維持するために、クラウドに転送されるデータの効率的でスケーラブルな安全性の確保を含む、包括的なITセキュリティー・アプローチを採用する必要があります。

これまで、IT組織はセキュリティーに対してオンプレミス・セキュリティーのイメージしか持っていませんでした。データセンターのエントリー・ポイントにある物理的なセキュリティーやサーバーと機器のアクセス制限などです。ファイアウォール、侵入防御システム、フルディスク暗号化、アプリケーションとデータベースの強化、ロールベースのアクセス制御など、さまざまなセキュリティー・エレメントにより、重要なデータ・リポジトリーがセキュリティー保護されて、暗号化されます。しかし、安全な場所から離れて、データセンター間を転送されるデータは、攻撃や漏洩に対して脆弱です。データがサードパーティーのネットワークや複数のサービス事業者のネットワークを経由する場合など、単一の組織がデータを完全に制御できない状況では問題がさらに複雑になるため、セキュリティーの確保がさらに難しくなります。

データセンター間の転送中データのプロテクションには暗号化を使用できますが、検討対象となるソリューションは多岐にわたります。それぞれの暗号化ソリューションには独自のメリットと課題がありますが、最高のソリューションが満たすべき条件は、導入と管理が容易で、拡張性が高く、効率的であることです。

セキュリティーをアプリケーション・レイヤーまたはネットワーク・インフラのいずれで実現?

IT組織が暗号化ソリューションを実装するときには、通常はアプリケーション・レイヤーでプロテクションを試みるか、ネットワーク・インフラに組み込まれた暗号化を使用します。アプリケーション・レイヤーのセキュリティーでは、ホストの装置とアプリケーションの両方をプロテクトする必要があるため、ほとんどのアプリケーション・レイヤー・セキュリティー・フレームワークはデータセンター内にあります。また、アプリケーション（ウェブ・ブラウザーやEメール・クライアントなど）とサーバー間の通信をプロテクトするTransport Layer Security（TLS）などのソリューションは、一般的にはクラウド経由またはデータセンター間の通信においてアプリケーション間のセキュリティーに対応しません。

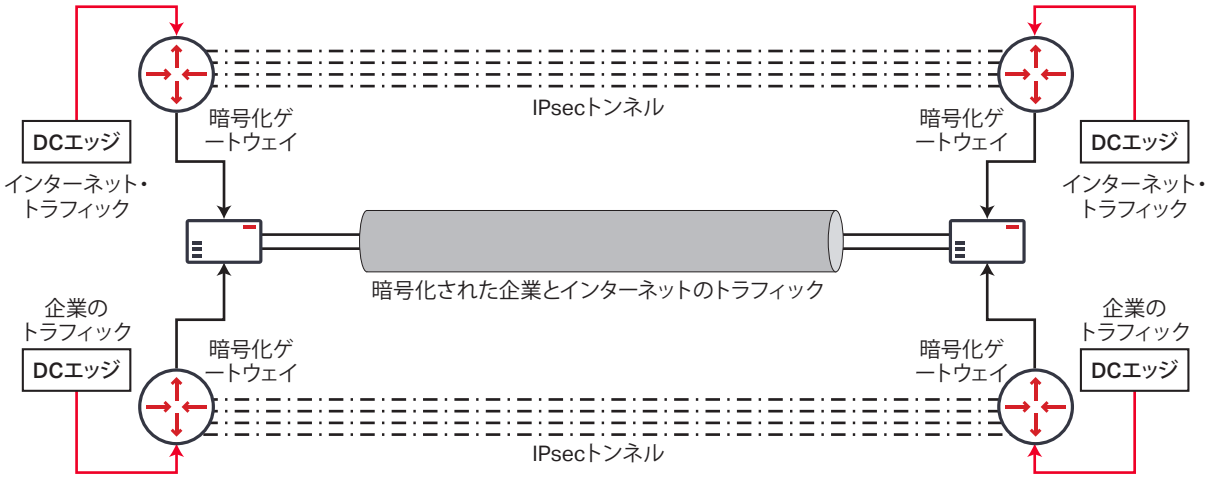

図2. オーバーレイによってパケット・レイヤーのすべてのトラフィックをプロテクト（論理ビュー）

複数のデータセンター間に、アプリケーション間のセキュリティーを確保する共通のフレームワークを構築することは困難であるため、多くの組織はネットワーク・インフラがその課題を解決することに注目しています。

ネットワーク・インフラの使用には独自の課題があり、インフラ・レイヤーでネットワークをプロテクトすることにより、ネットワーク・アーキテクチャーが非常に複雑になる可能性があります。データセンター間には膨大な量のトラフィック・フローがあり、すべてのトラフィックを100G以上の複数の接続全体でプロテクトすることは運用面から見て煩雑であり、簡単に設計およびスケーリングすることができません。

選択できるオプションの1つに、暗号化されたVPNゲートウェイのオーバーレイを使用して、パケット・レイヤーでトラフィックをプロテクトする方法があります（図2）。この方法では、プロテクトする必要があるリンクごとに、コストがかかる専用の暗号化ゲートウェイ装置を用意しなければなりません。このモデルでは、トラフィックが送信元/宛先の1組のIPペアに限定され、中間のルーターがマルチホップパス用に最も外側のIPsecヘッダー情報を使用することができません。このオーバーレイの手法ではトラフィックの変動に対応できず、等価コスト・マルチパス（ECMP）とリンク・アグリゲーション・グループ（LAG）のパスが切断されます。さらに、効率的にスケーリングされず、レイテンシーが増加します。帯域要件が増大して、データ・フローがよりメッシュ化されると、暗号化ゲートウェイでより高速なポートが必要になり、コストが大幅に増大します。

暗号化されたVPNゲートウェイのオーバーレイを使用してクラウドをプロテクトする手法には、主に次のような欠点があります。

- ネットワーク・アーキテクチャー、設計、エンジニアリングが複雑である
- データセンター間のトラフィックの運用と管理に専門的なスキルが必要である
- 効率的にスケーリングできない
- データセンター間でレイテンシーが増大する
- パケット・レイヤーでの暗号化の手法により、全体的なパケット・スループットが低下する
- モニタリング、トラブルシューティングをはじめ、運用面で課題がある
- 暗号化ゲートウェイ装置が高コストである

前述したように、トラフィック・フローが増加するにつれ、暗号化ゲートウェイにはより高速なポートが必要になります。このパケット・ベースのアーキテクチャーはスケーリング能力が低く、暗号化装置が非常に大型化してコストが増大し、データセンター間の暗号化リンクで高速なスループットを確保するのが容易ではありません。このようなスケーラビリティーの課題を解決し、トラフィック負荷に伴って増大する専用の暗号化ゲートウェイ装置のコストを削減するために、組織はトラフィックのプロファイリングを試みることができます。プロファイリングが完了すると、必要に応じて暗号化ゲートウェイまたは非暗号化ゲートウェイを使用して、トラフィックを暗号化パスと非暗号化パスに分類できます（図3）。この試みでは、暗号化が必要なトラフィックのみを暗号化ゲートウェイに送信して、その他のすべてのトラフィックを非暗号化ゲートウェイにオフロードすることで、スケーラビリティーの問題を軽減できます。

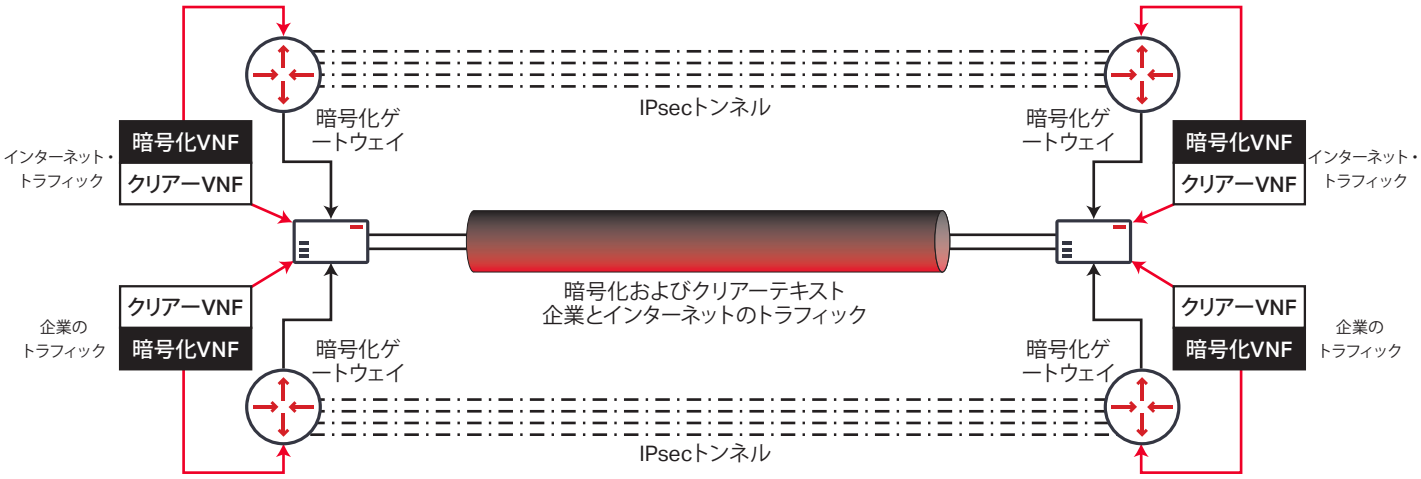

図3. 暗号化ゲートウェイのコストを削減するトラフィック・プロファイリング（論理ビュー）

しかし、トラフィック・プロファイリングにも課題があります。トラフィックの暗号化の有無を正確に判別するには、煩雑な作業が必要です。企業が十分な理解に基づいて、自社のデータを正確に分類することはほとんど不可能です。また、トラフィックを正確に識別できなければ、機密データをプロテクションなしで転送してしまう可能性があります。アプリケーションの目的やパラメーターは頻繁にアップデートされ、トラフィック・プロファイルがそれらの変更と常に同期されていない限り、機密データがプロテクトされていない経路で転送される可能性があります。

暗号化ゲートウェイと非暗号化ゲートウェイによってトラフィック・プロファイリングを使用する手法には、主に次のような欠点があります。

- ネットワーク・アーキテクチャー、設計、エンジニアリングが複雑である
- データセンター間のトラフィックの運用と管理に専門的なスキルが必要である
- 暗号化と非暗号化を分類するトラフィック・プロファイリングのエラー率が高い
- アプリケーション・プロファイルとトラフィック・プロファイルをアプリケーション利用の経時的な変化に同期させる必要がある
- ネットワーク・ハードウェア上に通常/クリアーと暗号化のルーティング・インスタンスを設計および実装する作業が複雑である
- データセンター間のレイテンシーが増大する
- パケット・レイヤーでの暗号化の手法により、全体的なパケット・スループットが低下する
- 暗号化ゲートウェイ装置のコストが高い

このような特性を持つトラフィック・プロファイリングをグローバル・レベルまでスケーリングすることは極めて難しく、長期にわたって維持することは容易ではありません。トラフィックを適切にプロテクトするために、新規/既存のアプリケーションおよびデータソースのトラフィック・プロファイルをこまめにアップデートする必要があります。また、トラフィック・プロファイリングを成功させるには、アプリケーション開発者、セキュリティー・エンジニア、システム管理者、ネットワーク管理者の間で絶え間なく緊密に協力する必要があります。

スケーラビリティーと実装の複雑さの点では、パケット・レイヤーの暗号化の両方の手法に欠点があります。幸い、光レイヤーで転送中のトラフィックを暗号化することにより、複雑さを低減して、スケーラビリティーを向上させる新しいオプションがあります。

24時間365日のデータ・セキュリティー・ソリューション

光レイヤー暗号化：シンプルでセキュアなアプローチ

機密データのみをプロテクトするために、リソースを消費してトラフィックをプロファイリングして分離するのではなく、すべてのデータにプロテクションが提供される、実装が容易な暗号化ソリューションとして光レイヤーに注目が集まっています。レイヤー1、つまり光レイヤーの暗号化は、それを実現します。光レイヤーの暗号化ではOTNペイロード全体が暗号化されるので、すべてのメッセージ、ヘッダー、上位レイヤーからの通信データの安全性が確保されます（図4）。

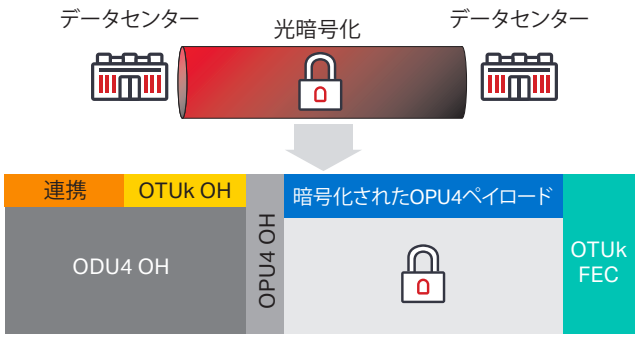

図4. レイヤー1暗号化によりすべてのトラフィックをプロテクト

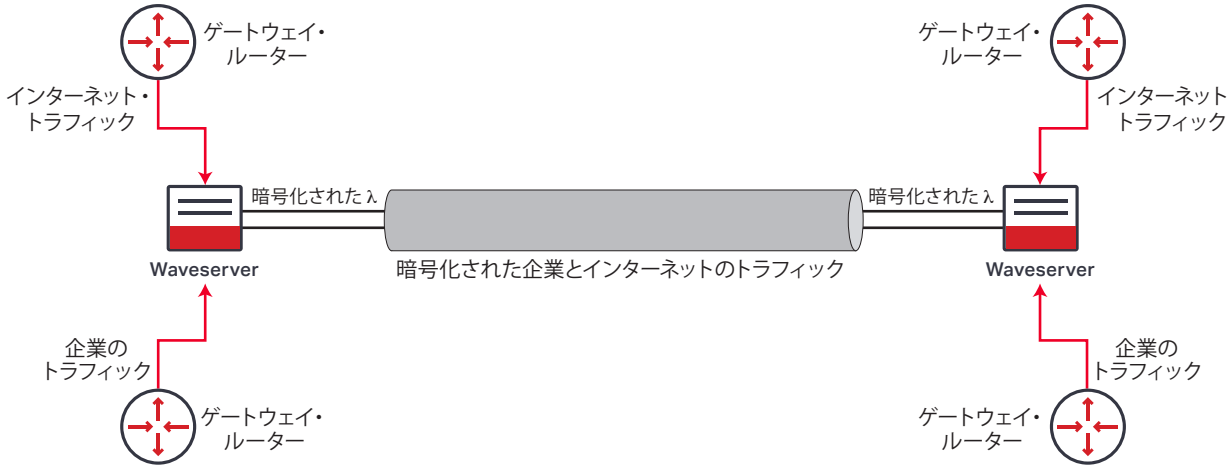

図5. 光レイヤーのすべてのトラフィックをプロテクト（論理ビュー）

光レイヤーでの暗号化により、ネットワーク・アーキテクチャーが簡素化されます（図5）。ゲートウェイ・ルーターは、トラフィックの一括暗号化を行うために、トランスポート装置（ここではWaveserer®）にトラフィックを直接送信します。高価な暗号化ゲートウェイは不要であり、暗号化対象のトラフィックを識別するトラフィック・プロファイリングも必要ありません。データセンターから伝送されるすべてのトラフィックが、高速スループットによりワイヤースピードで暗号化されます。

レイヤー1暗号化は、次のようなメリットを提供します。

- **トラフィックを暗号化するための追加のVPN要件が不要** — レイヤー1暗号化は、全トラフィックを暗号化するソリューションであり、暗号化VPN/非暗号化VPNの送信を判別するトラフィック・プロファイリングは必要ありません。すべての通信の安全性が確保されます。
- **無視できる程度のレイテンシー** — レイヤー1で暗号化を行う場合に増大するレイテンシーはナノ秒からマイクロ秒の単位であるのに対し、IPsecやアプリケーション・レイヤーの暗号化など、上位レイヤーで暗号化を行う場合に増大するレイテンシーは数百ミリ秒に上ります。
- **高速スループット** — トランスポート・レイヤーのペイロードのみが暗号化されるため、ルーターやスイッチ上のパケット・レイヤーのスループットに影響しません。レイヤー1のワイヤースピード暗号化ソリューションは、トラフィックの暗号化で高速スループットを提供します。
- **構築、設計、運用が容易** — レイヤー1暗号化ソリューションは、メトロまたは長距離ネットワーク全体にDWDM伝送を提供するために使用するオプティカル・トランスポート・システムに組み込まれているため、追加の暗号化アプライアンスは必要ありません。
- **マルチプロトコルのサポート** — レイヤー1は、イーサネット、IP、SONET/SDH、ファイバーチャネルなどの複数タイプのトラフィックをサポートするため、必要な各種暗号化アプライアンスの台数が減り、1つのプロトコル（IP）に限定されるIPsecのようなオプションに対するプロトコル・サポートが向上します。

レイヤー1暗号化へ移行することで、クラウドの安全性を確保するシンプルなソリューションを利用できるようになります。レイヤー1暗号化により、プロテクトされたリンク全体ですべての転送中データの一括暗号化が有効になります。レイヤー1暗号化のもう1つのメリットは、最下位レイヤーで「キャッチオール」として使用できることです。セキュリティー組織は必要に応じて、規制準拠または包括的なセキュリティー計画の一環として上位レイヤーの暗号化ソリューションを引き続き開発して設計できます。ただし、上位レイヤーでセキュリティー侵害が起こった場合でも、データは光レイヤーで暗号化されます。

グローバル・セキュリティー・ポリシー開発の進捗状況に応じて、包括的なセキュリティー計画を設計するオプション、またはキャッチオールとしてレイヤー1暗号化を追加するオプションを選択できます。

CienaのWaveLogic Encryptionソリューション

Cienaは、データがリスクのあるプロテクトされていないリンクを伝送されないように、レイヤー1暗号化を提供して、AES-256暗号化アルゴリズムによってデータを確実にプロテクトします。さらに、攻撃者が物理的なメディアにアクセスして、ファイバーにタップを付けようとすると、すべてのデータが暗号化されて利用不可になります。

CienaのWaveLogic Encryptionは、オプティカル・トランスポート・ネットワーキング装置に統合された実装が容易なワイヤースピード光暗号化ソリューションです。このアプローチでは一度設定すれば後は放っておけるので、暗号化は常時稼働し、すべての転送中データを常時プロテクトします。これにより、ヒューマン・エラーによって機密データが暗号化されていないネットワークに送信される状況を回避できます。

Cienaのソリューションは、楕円曲線暗号（ECC）などの最新の公開鍵暗号アルゴリズムをサポートするFIPS認定のAES-256暗号化エンジンを提供します。WaveLogic Encryptionは、コヒーレントWDMインターフェイスを使用して、Cienaの6500 Packet-Optical Platform上とCienaのスタッカブル相互接続プラットフ

ォームのWaveserverファミリー上で利用できます。コヒーレントWDMインターフェイスは、100G QPSK、150G 8QAM、200G 16QAM、単一キャリア400Gなどのさまざまな回線レートでワイヤースピードの暗号化を提供するようにプログラムできます。

Cienaの6500では、マックスポンダー・ベースのオールインワンの10G暗号化カード・ソリューションを使用するか、暗号化機能を備える100G/200Gライン・モジュールをクライアント・インターフェイス・カードとペアリングすることができるので、特定のトラフィック・ニーズに柔軟に対応できます。また、Waveserverにより、最大400GのAES-256ワイヤースピード暗号化容量と、10GE、40GE、100GEクライアントの混成をサポートする柔軟性をわずか1RUの筐体で実現できます。100GEのクライアント・インターフェイス向けに最適化されたWaveserver Aiを使用すると、単一のラックユニットで暗号化容量を最大1.2Tまで拡張できます。

Cienaのコヒーレント・トランスポートに組み込まれたライン側のプログラマビリティーにより、すべてのアプリケーション要件に合わせて回線容量を最適化し、メトロ、リージョナル、長距離ネットワーク全体で転送中データの安全性を確保できます。これにより、距離または基盤となる光回線システムに関わらず、データセンター間を安全に接続することができます。

6500とWaveserverは両方とも、クラウドの安全性を確保するために、上位レベルのアプリケーションやIPベースのインフラ・ソリューションに伴う複雑さを生じさせることなく導入できます。光ファイバー・ネットワーク全体に分散される機密情報や、データ・セキュリティーを義務づける法令や規制が増えているため、現在のクラウド・ベース通信には、サーバーのセキュリティーや保管データの暗号化だけでなく、転送中データの強固な暗号化ソリューションを含むITセキュリティー・アプローチを導入する必要があります。

手間のかからない暗号化。詳細を見る。

まとめ

包括的なセキュリティー計画は、特にデータセンター間のアプリケーション間通信を検討している場合、簡単には展開できません。データセンター間でデータを安全に伝送する手段として、多くの組織がネットワーク・インフラに注目しています。一方、レイヤー3でネットワーク暗号化を提供する方法は、コストがかかり、スケーリングが困難です。光レイヤーの暗号化は第1レベルの防御を提供し、実装も容易です。プロトコルに依存せず、さまざまなトラフィック・タイプをサポートします。高負荷時でもスループットを低下させずにワイヤースピードの暗号化を提供し、レイテンシーをほとんど増大させません。レイヤー1暗号化は、データセンター間を伝送される転送中データをプロテクトするための費用対効果の高い方法を提供します。CienaのWaveLogic Encryptionソリューションは、優れた柔軟性とセキュリティーを兼ね備え、運用と管理が容易です。費用対効果が高く、大容量で、ワイヤースピードの暗号化を提供し、街角を越え、都市を越え、国境を越え、海を越えて、データセンター間の通信を常時プロテクトします。

Cienaコミュニティーへアクセス
疑問を解決する