

# Thunder CFW IPsec VPN

## サイト間IPsec VPNによる大容量のトラフィック暗号化

### データプライバシーの課題

盗聴やデータ盗用の防止、そしてコンプライアンスへの対応のために、あらゆる規模の企業がIPsec VPNを使用しています。IPsecは、IPネットワークを介してデータを転送するコスト効率に優れた安全な方法を提供します。

IPsecは成熟した広く普及しているテクノロジーですが、クラウドコンピューティングなどの新しいネットワークパラダイムや増大する帯域幅の要件によって、大企業と大手サービスプロバイダーはVPN戦略の見直しを余儀なくされています。結果として、次のことが可能なVPNアーキテクチャーを開発する必要性に直面しています。

ネットワークを管理するスタッフにとって、ネットワークトラフィックの状態、関連するトラフィックの種類、ネットワーク通信の発生元に関する情報は重要です。そのような情報は、ネットワークの拡張の必要性を予測したり、ネットワークの問題を分析するときにも活用できます。

- これまでにない高いレベルのIPsecスループットのサポート
- 高可用性と迅速な拡張を実現するBGPルーティング
- クラウド環境における新しいIPsecトンネルとゲートウェイのオンデマンドな確立
- 電力消費とラックスペースの要件を最小限に抑え、データセンターを効率化

組織には、信頼性の高いIPsec接続性を提供することが裏付けられており、かつ既存のルーターやIPsec VPNゲートウェイと相互運用できるソリューションが必要とされています。

### データ保護の必要性

機密データは通常、リモートサイト間で転送されますが、現在ではパブリッククラウドからプライベートクラウドに転送する組織が増えています。そのため、データを盗聴とハイジャックから保護することは、多くの企業、政府機関、サービスプロバイダーにとって必要不可欠になっています。転送する機密データを保護するには、サイト間VPNソリューションを導入する必要があります。

IPsecを使用すると、データ送信元の認証、アクセス制御、データ再生防止によってIPパケットが保護され、強力な暗号化によってデータの機密性が保護されます。

A10 Networks® Thunder® Convergent Firewall (CFW) の提供するハイパフォーマンスなIPsecソリューションは、既存のネットワークインフラストラクチャーへの容易な導入・統合を行うことができ、SSLインサイトやファイアウォールなど、データセンターのアプリケーションを保護する他のセキュリティ機能とともに一元管理できます。

### 課題

企業とサービスプロバイダーは、通信を保護するため迅速にデータを暗号化し、オンデマンドでVPNトンネルのキャパシティを拡張することが必要。

### ソリューション

A10のソリューションにより、企業やサービスプロバイダーは他の重要なセキュリティとアプリケーション配信のコンポーネントに統合されたハイパフォーマンスなIPsec VPNソリューションによってデータセンターのスペースを削減するとともに、データプライバシーを確保可能。

### 利点

- ハイパフォーマンスなIPsec VPN、トラフィック検査、ステートフルファイアウォール機能を提供
- 卓越したスピードでデータを暗号化
- ラックスペースと電力の要件を低減
- 新しいVPNゲートウェイをオンデマンドで開始し、キャパシティを拡張
- ハイパフォーマンスなハードウェアベースのIPsec暗号化でセキュリティを確保し、インターネット経由でリモートサイト間を安全に接続

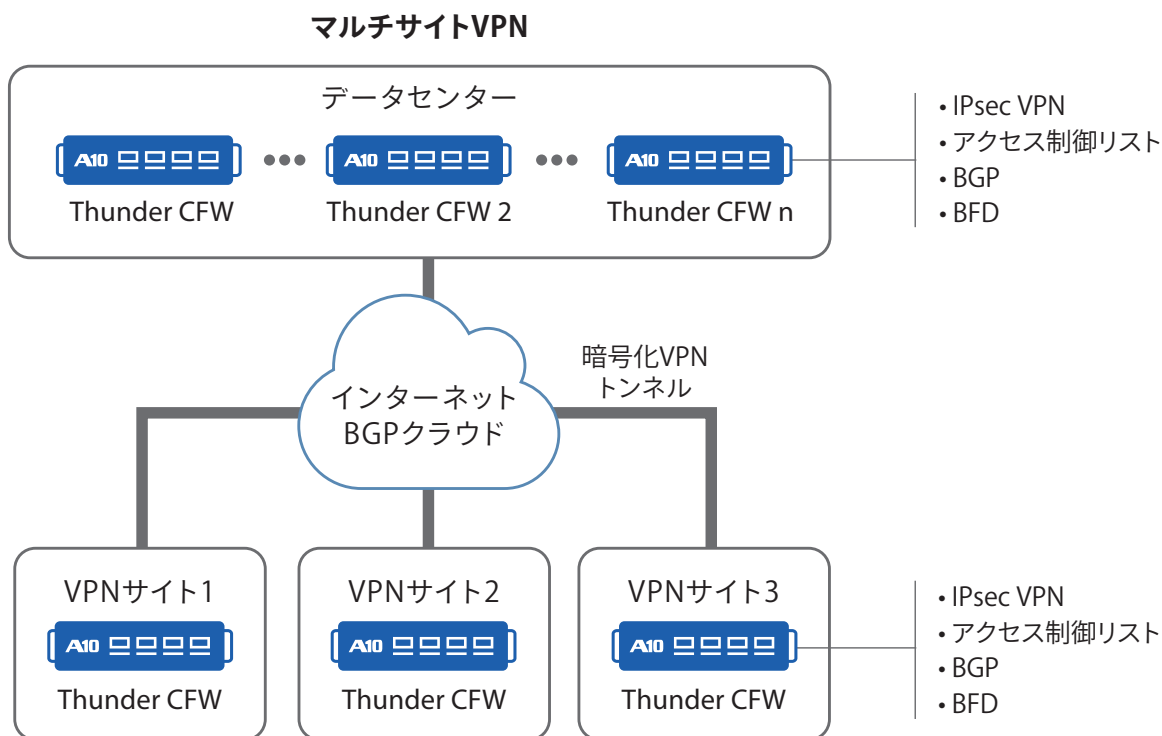


図1: Thunder CFWはBGPクラウドを介して複数のVPNサイトと接続可能

## 高速なIPsec暗号化通信

A10 Thunder CFWはIPsec暗号化機能を搭載しているため、企業やサービスプロバイダーは大規模なVPN環境を構築できます。Thunder CFWプラットフォーム当たり最大20,000のVPNトンネルに対応し、幅広い暗号化アルゴリズムとデータ整合化手法がサポートされているため、組織では既存のVPN機器とThunder CFWを併用することも、Thunder CFWアプライアンスを利用して新しいVPNネットワークを構築することもできます。

Thunder CFWはIPsec VPNだけでなく、高度なサーバー負荷分散、ネットワークアドレス変換(NAT)、IPv4およびIPv6ルーティング、データセンターとGi/SGiファイアウォール、SSLインサイト、セキュアWebゲートなど、さまざまなトラフィックセキュリティ機能をサポートしています。幅広いネットワーク機能が利用可能なため、多数のアプライアンスの導入と管理が必要なく、複雑なネットワーク設計をサポートして、リモートのリソースへのアクセスをきめ細かく制御できます。IPsecに加え、これらの機能もすべて、Thunder CFWに標準装備されています。

## 高可用性と迅速な拡張

VPNは、データ移行、災害復旧、リモートユーザーアクセス、データセンターとクラウドネットワークの接続などのビジネス上の重要な機能を多くの組織で果たしています。用途を問わず、VPNはビジネスに欠かすことができないため、常時使用可能でなければなりません。

Thunder CFWは、クラスターリング、高可用性、動的なルーティング機能によって、IPsec VPNルートのアップタイムを最大限に高めるだけでなく、サーバーとアプリケーションへの接続性も保証します。Thunder CFWでは、次のような高可用性および拡張機能が提供されています。

- **ルート監視とフェイルオーバー**

A10 Networksによって強化された仮想ルーター冗長化プロトコル実装(VRRP-A)を使用するThunder CFWは、ルートとVPNゲートウェイの障害を監視し、パッシブなThunder CFWアプライアンスにすばやくトラフィックをフェイルオーバーできます。VRRP-Aはクラスター当たり最大8台のアプライアンスをサポートしており、応答しないサービス、サーバー、アプリケーションを検知し、インフラストラクチャーの障害を特定できます。A10 Networks Virtual Chassis System (aVCS®)によって、

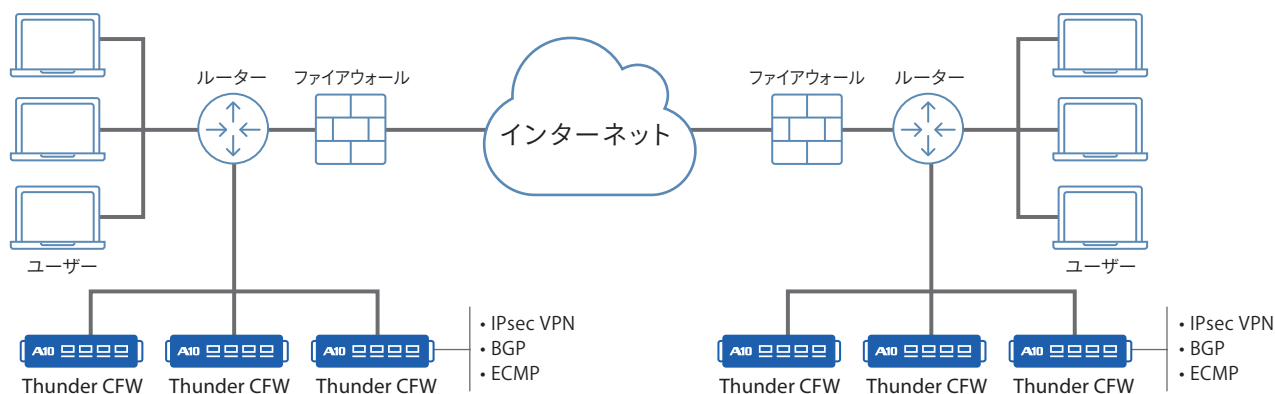


図2: ユーザーは、Thunder CFWアプライアンスを介してリモートVPNサイト宛のトラフィックを転送し、他のすべてのトラフィックを直接インターネットに送信可能。

複数のA10デバイスが単一の仮想シャーシとして機能できるため、シングルポイントからの制御と一元的な統計情報の入手が可能になります。

#### • インテリジェントなルーティングによるVPNのキャパシティ拡張

Thunder CFWは、BGP (Border Gateway Protocol) ルーティングをサポートしています。したがって、BGPルーターがIPsec VPNトンネルを介して通信できるだけでなく、Thunder CFWアプライアンスを追加するだけでIPsecのキャパシティを強化できます。BGPを使用するThunder CFW環境は、複雑なネットワーク設計やハードウェアのフォークリフトアップグレードの必要なく拡張して、テラバイト級の帯域幅の要件に対応できます。また、Thunder CFWアプライアンスを追加することによってIPsecのスループットを高められます。VRRP-AはBGPとの統合によって、ルートをインジェクトし、スムーズなルートのフェイルオーバーが行えます。Thunder CFWは、高速なパス障害検知とルート統合のためにBFD (Bidirectional Forwarding Detection) もサポートしています。

#### • 複数のパスを介した負荷分散による帯域幅の統合

Thunder CFWでは、ECMP (Equal-Cost Multipath) ルーティングを活用して、IPsec VPN帯域幅を総合的に拡張できます。ECMPとBGPを組み合わせることで、ルーターは複数のネットワークルートを同時にサポートできるため、Thunder CFWは複数のパス間でトラフィックを負荷分散し、総合的なVPNキャパシティを拡張できます。

## ハイパフォーマンスアーキテクチャー

Thunder CFWは、独自のソフトウェア/ハードウェア設計のメリットを駆使して、卓越したIPsecパフォーマンスを実現します。また、A10 NetworksのAdvanced Core Operating System (ACOS®)によって、Thunder CFWアプライアンスを強化できます。マルチコアCPUアーキテクチャーのパフォーマンスを最大限に高めるためにゼロから構築されたACOSは、CPUコアが追加されるとコンピューティング処理をリニアに拡張することができ、コンパクトなフォームファクターで卓越したパフォーマンスを提供します。

ACOSは、スケーラブルな対称型マルチプロセッシング (SSMP) を使用することによって、スーパーコンピューターの並列処理技法を取り入れるとともにマルチコアアーキテクチャーのパフォーマンスを最大限に高めます。マルチコアアーキテクチャー向けに最適化された拡張性の高い64ビットオペレーティングシステムを通じて、Thunder CFWアプライアンスは比類のないIPsec VPNパフォーマンスを実現します。

一部のThunder CFWハードウェアモデルには、IPsec暗号化速度を高速化する専用セキュリティプロセッサが搭載されています。ラックマウント可能なアプライアンス1台で複数のセキュリティプロセッサをサポートするThunder CFWは、煩雑で非効率なシャーシベースシステムの導入の必要なく高速なIPsec暗号を実現します。

Thunder CFWの高いパフォーマンスとデータセンター向けに最適化された設計により、プロビジョニングするアプライアンスの台数を削減することが可能になり、結果として資本/運用コストだけでなく、データセンターのラックスペースおよび電力コストも削減できます。

## まとめ

組織は、信頼性の高いIPsec接続性を提供することが実証されており、既存のルーターおよびIPsec VPNゲートウェイと相互運用できるソリューションを必要としています。Thunder CFWのIPsec VPN機能によって、高速でのトラフィックの暗号化や、BGPルーティングとオンデマンドのVPNプロビジョニングをサポートすることができます。Thunder CFWのIPsec VPNテクノロジーを利用すると、以下のことが可能です。

- A10の64ビットACOSプラットフォームと専用セキュリティプロセッサによる、増大するIPsecスループット要件への対応
- IPsec VPN、データセンター、Gi/SGiファイアウォール、ネットワークアドレス変換(NAT)、IPv4およびIPv6ルーティング、SSLインサイト、セキュアWebゲートウェイ、サーバー負荷分散およびその他のセキュリティ機能を単一のデバイスに統合
- Thunder CFWのデータセンター効率の高い設計による、ハードウェア、運用、保守コストの削減
- パブリック、プライベート、ハイブリッドクラウドのプロビジョニングとBGPネットワークの要件サポート

## A10 Networks / A10 ネットワークス株式会社について

A10 Networksは、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Webサービス事業者まで7000社以上のお客様に導入いただいております。ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは2004年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。

A10 ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワークワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

- URL : <https://www.a10networks.co.jp/>
- X (旧 Twitter) : <https://twitter.com/a10networksjp>
- Facebook : <https://www.facebook.com/A10networksjapan>

Learn More

About A10 Networks

お問い合わせ

[A10networks.co.jp/contact](https://www.a10networks.co.jp/contact)

A10ネットワークス株式会社

[www.a10networks.co.jp](https://www.a10networks.co.jp)

©2024 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他の各国におけるA10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。 [www.a10networks.com/a10-trademarks](https://www.a10networks.com/a10-trademarks)

Part Number: A10-SB-19153-JA-02 JUN 2024