トンネルフリー SD-WAN のセッションインテリジェンス

セッションスマートネットワーキングはどのようにしてトンネルの限界を克服するのか

ホワイトペーパー

目次

概要

ネットワーク管理者やエンジニアは、SD-WAN（Software-Defined WAN）を実装することであらゆる規模の分散型企業環境に対応します。こうした SD-WAN は、一般的に IPsec、GRE（Generic Routing Encapsulation）、VXLAN（Virtual Extensible LAN）などのトンネリング技術を使用して構築されます。

トンネルベースネットワーキングは、SD-WAN に対して一定のセキュリティを提供しますが、その一方で複雑さを大幅に増大させ、ネットワークリソースを浪費します。その結果、パフォーマンスが予測不可能になり、エクスペリエンスの低下につながります。

トンネルフリーでセッションインテリジェントな SD-WAN は、リアルタイムか非同期かを問わず、すべてのアプリケーションでユーザーと運用担当者のエクスペリエンスを向上させます。Juniper® セッションスマートネットワーキングを採用したジュニパーの Mist AI™ ドリブン SD-WAN は、トンネルベースの SD-WAN よりも高いパフォーマンス、拡張性、安全性を提供し、よりシンプルに運用できます。

さらに、セッションスマートネットワーキングとともに Juniper Mist ™ WAN Assurance を利用すれば、ネットワークユーザーと運用担当者のエクスペリエンスが飛躍的に向上します。

はじめに

トンネルベースのネットワーキングは、WAN やインターネットのセキュリティを向上させる必要性から生まれました。急増する接続需要に対応するため、プライベートルーティングネットワークがステートレスかつコネクションレス型で構築され、増え続けるトラフィックの波を全世界に向けて配信するようになりました。このような大規模なワークロード環境下では、ネットワークエッジでセキュリティを処理するほうが好ましい選択肢でした。

パブリックネットワークが高価値のビジネスアプリケーションに対して使用されることが増えたことから、ルーティングファブリック自体に組み込まれたセキュリティの強化が必要になりました。この目的のために開発されたのが、トンネリングプロトコルです。中でも IPsec は、パケットを認証し暗号化して IP ネットワーク上で安全に送信するために開発されました。

Software-Defined Networking（専用のハードウェアを作成するよりも迅速な開発が可能）やその後の SD-WAN の成長に伴い、IPsec はトラフィックを安全に処理する方法として費用対効果が高いことが実証されました。企業、ユーザーグループ、アプリケーションのトラフィックが非同期（データベースアクセスなど）かつリアルタイム（テレフォニーなど）であるダイナミックなマルチパス環境において特に、IPsec は便利でした。

IPsec トンネルによって仮想化が行われ、より大規模で抽象的なマルチサイト、マルチクラウド接続を SD-WAN で処理できるようになりました。しかし、こうしたトンネルの急増は、運用の複雑さと帯域幅の非効率性という問題を引き起こしました。

トンネルベースネットワークのトレードオフ

トンネルは暗号化と認証によってセキュリティ要件を実現し、整合性チェックによって改ざん防止の手段を提供します。トンネリングプロトコルの標準化（特に IPsec、GRE、VXLAN）により、異種ネットワーク間の互換性が確保されます。トンネルは汎用性が高く、さまざまな用途に対応できます。

ただし、こうしたメリットには相応の代償も伴います。トンネルベースネットワーキングの主なメリットとデメリットを、表 1 に示します。

表 1：トンネルベースネットワークのトレードオフ

メリット	デメリット
暗号化により、攻撃者がデータを傍受してもその内容を読み取ることや理解することはできません。	オーバーヘッドによる**パフォーマンス低下**は 30 ～ 40% またはそれ以上に達します。
認証により、許可されたデバイスのみが接続できるようになります。	**重度なカプセル化**により、ペイロードが小さくなり、グッドプットが低下します。
整合性チェックによる**改ざん防止機能**により、ペイロードの改ざんを防止します。	トンネルの管理が過度に**複雑**になります。
デバイスの互換性、および OS の相互運用性と独立性は維持されます。	各ベンダーが導入したトンネル間で**互換性の問題**が発生します。
さまざまなアプリケーションやサービスがサポートされています。	特にリアルタイムのビデオ通信で**品質が制限**されることがあります。

カプセル化による追加オーバーヘッドの発生が、トンネルベースのネットワークでパフォーマンスが低下する主な原因です。パケットは指定された MTU（最大送信単位）サイズ内に収まる必要があるため、カプセル化が過剰に行われると、パケットあたりのペイロードが小さくなります。パフォーマンスの低下は、高帯域幅のアプリケーションやリソースが限られたデバイスで特に顕著にみられる可能性があります。

トンネルはまた、多数の暗号化アルゴリズムと認証方法を必要とします。セキュリティを強化するために鍵方式を用いて導入することが多く、導入先の規模が大きいと鍵基盤の管理が非常に複雑になります。

その上、標準化されたトンネリングプロトコルを使用している場合であっても、異なるベンダーが導入したトンネルの間で互換性に問題が生じます。トンネルは個別のセッションを数多く送信しますが、ネットワークからは 1 つの大きなセッションに見えます。

このような状況では、トラフィックを適切に分類することは非常に困難です。トラフィックのエンジニアリングをトンネルごとに行うことでのみ、ユーザーエクスペリエンスを改善することができますが、個々のアプリケーションはトンネル内に組み込まれているため、このような改善を行うにも限界があります。

SD-WAN の台頭とトンネル利用の継続

SD-WAN は、クラウドコンピューティングやビデオ会議、リモートワークなどの最新のビジネス手法に適しています。一方でこうしたビジネス手法が WAN を限界に追い詰めています。SD-WAN は従来の WAN よりも俊敏性に優れ、新しいアプリケーションやサービスをより迅速かつ簡単に設定できます。

SD-WAN は複雑さの解消にも役立ちますが、トンネルに依存している部分もあるため、その大半は非常に不安定です。各トンネルは、企業の本社と支社など、2 つのエンドポイント間の直接接続を確立します。ネットワーク上のすべてのサイト間でトンネルを確立するのは、時間がかかり、複雑化しやすくなります。

SD-WAN の規模に関しては、多くの場合、トポロジーの制約が最大の制限となります。すべてのサイト間の「n 乗」数のトンネルを管理するという複雑さを避けるには、ハブアンドスポーク型のトポロジーが必要です。 このトポロジーを採用すると、支社間でのリアルタイムのメディア送信を防ぐことができます（図 1）。

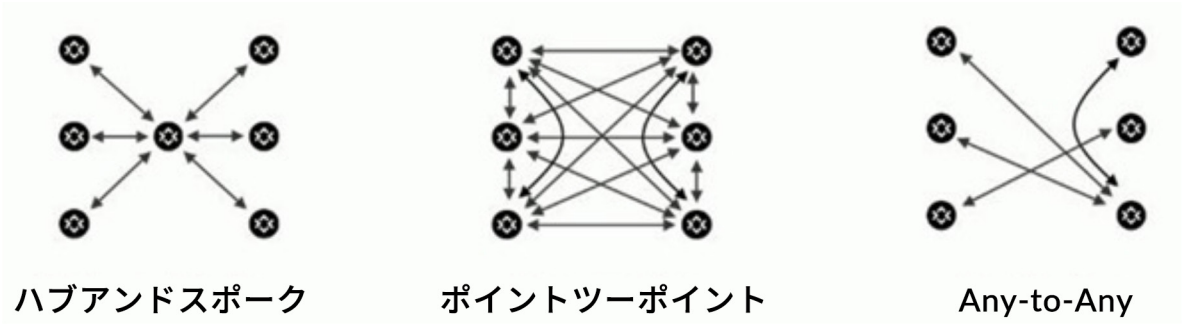

図 1：セッションインテリジェンスで解決するトンネルのトポロジー制限

ハブアンドスポーク型トポロジーの場合、余分なホップがあると非効率的な経路が発生し、多くの場合、ビデオ通話ができないほどの遅延が発生します。その代わりとして、ポイントツーポイントネットワーキングが考えられますが、これは拡張性が低く管理も困難です。

セッションごとに作成される Any-to-Any トポロジーであれば、これらの問題を回避し、予測可能で最適なパスを提供できます。このトポロジーは、トンネル管理のオーバーヘッドがなく、導入がはるかに簡単です。

フラグメント化も問題点の 1 つです。パケットがサポート可能なサイズよりも大きい場合、トンネルに入ると複数のパケットに分割され、反対側で再アセンブリされます。これを行うために、処理能力、メモリ、CPU リソースが消費されます（図 2）。

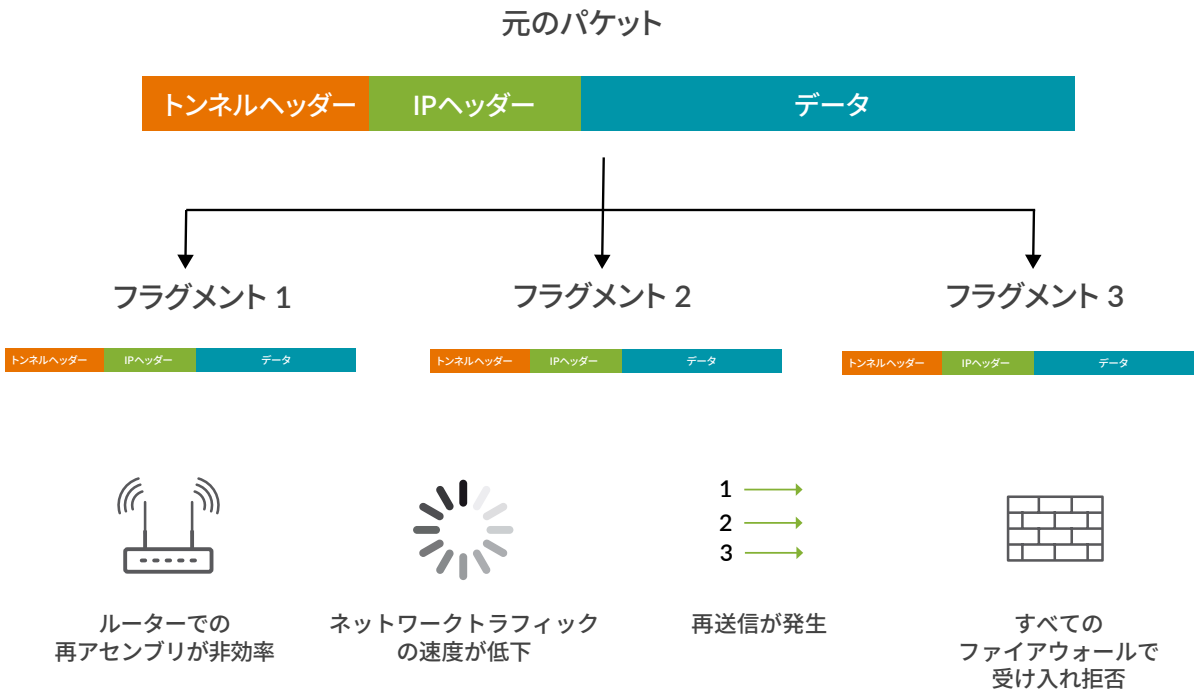

図 2：フラグメント化と再アセンブリの問題

このような非効率的でコストのかかる再アセンブリに加え、フラグメントが失われ、再送信が必要になることもよくあります。伝送時間が長くなると、スループットが低下し、拡張性が制限され、ユーザーエクスペリエンスが低下します。さらに、ファイアウォールが順序を逸脱した非初期フラグメントをブロックするため、さらなるドロップと再送信が発生することになります。

この 2 つの問題の詳細については、ACG Research のホワイトペーパーをご覧ください。この他にも、特に SD-WAN に関連しているトンネルに問題があります。アプリケーションの可視性の欠如や二重暗号化の非効率性などの問題です。

ジュニパーの Mist AI ドリブン SD-WAN

ジュニパーは、運用担当者とユーザー双方のエクスペリエンスを向上させるチャンスと捉え、より優れた SD-WAN の構築に着手しました。ジュニパーのトンネルフリーアプローチは、SD-WAN ルーティングにセッションインテリジェンスというメリットを導入しました。これにより、トンネルベースプロトコルが改善されると同時に、データの整合性、暗号化、認証が実現されます。

スループットの向上

ジュニパーの Mist AI ドリブン SD-WAN が提供する明らかなメリットとして、トンネルヘッダーのオーバーヘッドを除去し、より効果的で軽量な設計に置き換えることで、送信されるユーザーペイロード（グッドプット）が大幅に増加することによるスループットの向上が挙げられます（図 3）。

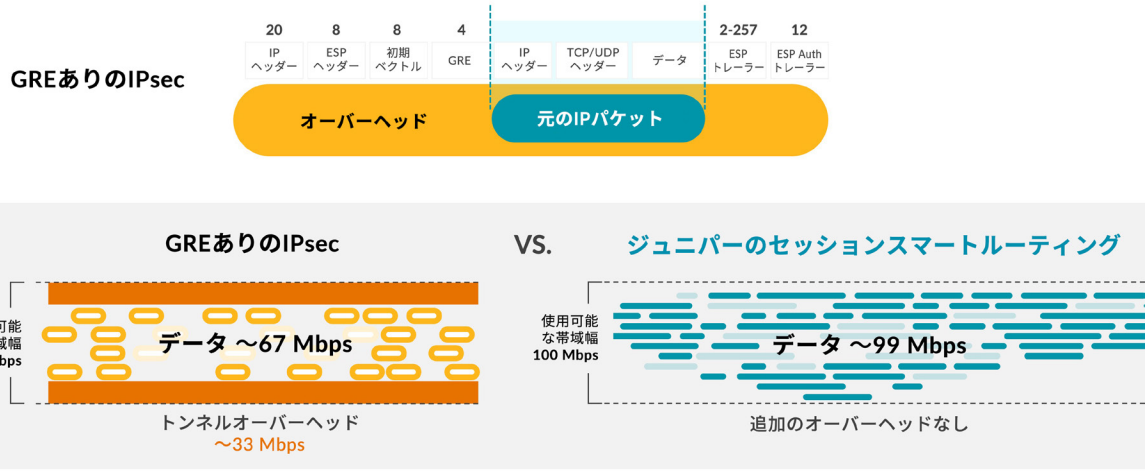

図 3：IPsec と GRE による帯域幅の無駄遣い

トンネルを必要としないため、IPsec や VXLAN ベースのネットワーキング方式に比べて 30% から 40% の節約が可能です。帯域幅の使用量はアプリケーションによって異なります。パケットサイズも要因の 1 つで、小さな音声パケットの場合、節約率は 100% に近くなります。

セッションスマートのメリット

ジュニパーの SD-WAN を支えるジュニパーセッションスマートルーターは、トンネルを使わず、セッション確立に必要な対称双方向接続の最初のパケットに小さなメタデータ Cookie を埋め込みます。このプロセスでは、ウェイポイントを使用してネットワークパス全体にわたってセッションをガイドします。ジュニパーのセッションスマートネットワーキングは、ゼロトラストのデフォルト拒否ルーティングモデルの採用により、従来のネットワークを上回るセキュリティを実現します。セッションを許可する明示的なポリシーがなければ、セッションは許可されません [1]。

セッションスマートネットワーキングは、テレフォニーから取り入れた基本原理によって生まれました。ユーザーが通話を開始し、受信者がそれを受けることで、セッションが構成されるという原理です。これこそまさに、ユーザーとアプリケーションが繋がる仕組みです。セッションインテリジェンスは、アプリケーションを認識し、個々のユーザーエクスペリエンスを保証します。この保証は、確実なフェイルオーバーと、ユーザーごとに適用される QoS ポリシーという形で提供されます。

逆に、トンネルベースのアーキテクチャでは、サービス品質（またはエクスペリエンス）はトンネルレベルでのみ評価され、それに基づいてのみアクションが実施されます。つまり、トンネル内のアプリケーションはすべて、同じように扱われます。しかし、トンネル内ではアプリケーションの要件が異なることが多く、さまざまな理由でパフォーマンスが低下する可能性があります。

そのため、トンネルベースの環境では、Microsoft 365、社内データベース、ビデオ電話アプリケーション（以上はあくまで例です）などにまたがる遅延、ジッター、損失などの属性の QoS 設定を変更しても、あまり効果はありません。これらのアプリケーションのどれか 1 つだけを調整しても、かえって別のアプリケーションのパフォーマンスが低下する恐れがあります。トンネルベースの SD-WAN は、アプリケーション単位やユーザー単位でアクションを実行することはできないため、アプリケーションのパフォーマンスを妨害するトラフィックを許可しないように設定することはできません。

[1]これについては、『セキュアベクトルルーティング』（インターネットドラフト版）および『セッションスマートルーティング - その仕組み』で詳しく説明しています。

一方、セッションスマートネットワーキングでは、アプリケーションごとの可視性が強化され、その細かさも向上します。両者の違いを図 4 に示します。

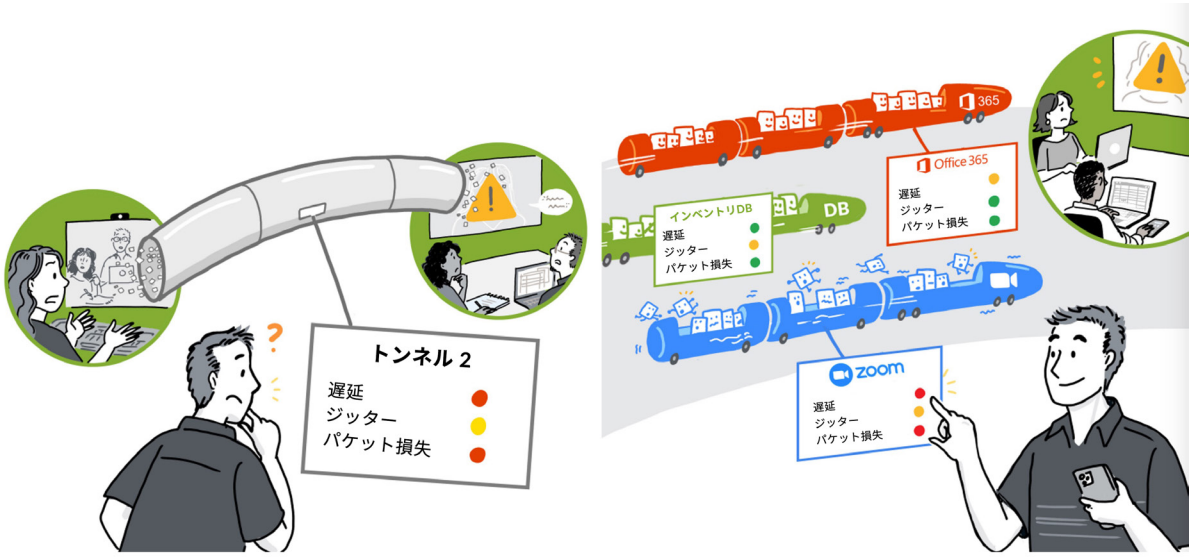

図 4：トンネルを使わずセッション上で運用

この環境では、アプリケーションの可視性と制御の調整がはるかにしやすくなり、すべてのアプリケーションで最高のパフォーマンスが得られます。

セッションスマートとMist AIの組み合わせ

前述したように、セッションスマートネットワーキングのトンネルフリーという性質は、ネットワークトラフィックのより詳細な可視化を可能にします。このように可視性が強化されることで、ルーターはより豊富なテレメトリを収集できるようになります。Juniper Mist WAN Assurance では、この豊富なテレメトリ情報が Mist AI エンジンに送信されることで、ネットワークの健全性に関する実用的なインサイトが得られるようになります。

セッションスマートの豊富なテレメトリとこのデータに基づいた Mist AI の実用的なインサイトの組み合わせは、非常に強力です。

WAN Assurance は、アプリケーションの問題やサーバーのレスポンスの低下など、ネットワークのパフォーマンスに影響を与える問題の根本的原因を明らかにします。セッションスマートが提供するテレメトリは、このようなインサイトの質を向上させ、エンドユーザーエクスペリエンスに影響が及ぶ前に IT 運用担当者が問題を発見して修正できるようになります。

メリットのまとめ

AI とセッションスマートを組み合わせるメリットのほかにも、セッションスマートネットワーキングには数多くのメリットがあります。

企業内では、セッションが極めて多数の規模へと拡張される可能性があります。たとえば、何千人もの従業員の一部、または大多数が、社内データベース、クラウドストア、ビデオおよびテレフォニーアプリケーション、チャットアプリケーション、ブラウザー、イントラネットポータル、または業務に関連しないアプリケーションに接続されているかもしれません。これらのアプリケーションのすべてまたは大半が単一のトンネルにバンドルされている場

合、アプリケーションのエクスペリエンスの品質を検知して改善することは不可能です。セッションスマートネットワーキングでは、セッションの規模を桁違いに拡張できます。

さらに、全体的なアプリケーションのパフォーマンスは実際には何倍も速くなります。ドロップしたパケットや順序を逸脱したパケットの再送がアプリケーションのパフォーマンスをさらに低下させる原因であるためです。こうした再送信が低減するため、お客様はアプリケーションのパフォーマンスが 900% くらい向上したと実感しています[2]。

まれなケースですが、めったに起こらないフラグメント化が発生すると、セッションスマートネットワーキングではメタデータシグナリングを利用して、フラグメント化されたトラフィックの再構成方法を受信する側に知らせます。パスに沿って MTU の問題を取り除くことで、より高いパフォーマンスの提供が可能になります。

その他の相違点の概要を表 2 に示します。

表 2：セッションスマートネットワーキングとトンネルベースの SD-WAN の比較

トンネルフリーのセッションインテリジェンス	トンネルベースの SD-WAN
数百万セッションまで拡張可能	**数千セッション**までしか拡張できない
効率的な接続を実現する**柔軟なオンデマンドメッシュアーキテクチャ**	トラフィックが行き来する**ハブアンドスポーク型アーキテクチャの適用**
最初のパケット以降はオーバーヘッドなし	**多くの帯域幅を消費**
トンネルが引き起こす余分なカプセル化がないため、**フラグメント化はめったに発生しない**	パフォーマンス低下の原因となる**フラグメント化**が発生
異種ネットワークでの**迅速なフェイルオーバー**	**フェイルオーバーの不足**：長いトンネル設定時間や不必要なバックアップトンネル
ハイパーセグメンテーションによる**セキュリティの強化**	フローを曖昧にすることで**セキュリティがすり抜けられる**
極めて簡素化された鍵の処理はシステムが完全に管理：セッションごとに 1 つの鍵を使用	**ローテーションと認証機関を用いた個別の鍵管理インフラストラクチャ**（PKI など）が必要
常に利用可能な**暗号化**、ただし二重暗号化はなし	**暗号化レベルは低く**、冗長な場合もある

二重暗号化は適応型暗号化オプションによって防止できます。このオプションは、暗号化されたトラフィックを識別し、暗号化されていないトラフィックについては、セッションスマートルーターを通じて暗号化することでセキュリティを確保します。

[2]『次世代石油ガス事業者ネットワークがデジタル変革を加速（英語）』を参照。

まとめ

セッションスマートネットワーキングを採用したジュニパーの Mist AI ドリブン SD-WAN は、トンネルフリーでセッションインテリジェントな SD-WAN を構築します。リアルタイムか非同期かを問わず、すべてのアプリケーションでユーザーと運用担当者のエクスペリエンスが向上します。セッションスマートを活用したジュニパーの AI ドリブン SD-WAN は、トンネルベースの SD-WAN よりも優れたパフォーマンス、拡張性、安全性を誇り、よりシンプルに運用できます。

メリットとしては、、帯域幅と複雑さの軽減、フラグメント化や二重暗号化の回避、ゼロトラストセキュリティ、シンプルな運用、迅速で信頼性の高いフェイルオーバーなどが挙げられます。

セッションスマートネットワーキングの豊富なテレメトリを Mist AI エンジンに取り込むと、さらなるメリットを得られます。WAN Assurance を利用すると、IT 部門は WAN ネットワークの健全性に関する実用的なインサイトを得ることができ、トラブルシューティングに要する時間が大幅に短縮されるため、ユーザーと運用担当者のエクスペリエンスが向上します。

リソース

ビデオ

- Simplified：セッションスマート活用の AI ドリブン SD-WAN
- セッションスマートテクノロジーの概要（SVR）
- 比較：ジュニパーの SD-Branch とトンネルフリー SD-WAN

ホワイトペーパーとソリューションブリーフ

- ACG Research：トンネルベースとトンネルフリーの SD-WAN
- セッションスマートルーティング：その仕組み
- AI ドリブンエンタープライズによるクライアントからクラウドまでのアシュアランス

インフォグラフィックコンテンツ

- トンネルフリーを推奨する 8 つの理由
- お使いのネットワークは「バッドプット」に悩まされていませんか？

ジュニパーネットワークスについて

ジュニパーネットワークスは、ネットワーク運用を劇的に簡素化し、エンドユーザーに最上のエクスペリエンスを提供することに注力しています。業界をリードするインサイト、自動化、セキュリティ、AI を提供する当社のソリューションは、ビジネスで真の成果をもたらします。つながりを強めることにより、人々の絆がより深まり、幸福、持続可能性、平等という世界最大の課題を解決できるとジュニパーは確信しています。

JUNIPER NETWORKS | Driven by Experience™

アジアパシフィック、ヨーロッパ、中東、アフリカ
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
電話番号：+31.207.125.700
FAX：+31.207.125.701

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話番号：888.JUNIPER（888.586.4737）
または +1.408.745.2000 | FAX：+1.408.745.2100
www.juniper.net

日本
ジュニパーネットワークス株式会社
東京本社
〒163-1445 東京都新宿区西新宿3-20-2
東京オペラシティタワー45階
電話番号：03-5333-7400
FAX：03-5333-7401
西日本事務所
〒530-0001 大阪府大阪市北区梅田2-2-2
ヒルトンプラザウエストオフィスタワー18階
https://www.juniper.net/jp/jp/

2000810-001-JP 2023年9月