

トンネルフリーのSESSION SMART SD-WANでリモートワーカーをサポート

リモートワークはより一般的になっただけでなく、緊急事態時には企業にとって不可欠なものに

課題

従来、VPNソリューションはIPsecまたはSSLトンネリングを基盤としていました。これらの技術は柔軟性に欠けるモデルをベースにしているため、複雑で拡張が困難で、リモートワークへの対応を難しくしていました。

ソリューション

Session Smart SD-WANは、俊敏性、セキュリティ、高品質のリモートユーザーエクスペリエンスを実現するうえで最適な、「どこにいても働ける」アーキテクチャを実現するサービス中心のファブリックを構築します。

メリット

- ユーザーエクスペリエンスとネットワークパフォーマンスを改善
- コンプライアンスを維持しながらセキュリティリスクを低減
- 豊富できめ細かなサービスとネットワーク可視化
- 簡素化された、サービス中心でトンネルフリーのアーキテクチャ

COVID-19のパンデミックを受けて、企業には、柔軟性があり安全で生産性の高いリモートワーク環境への対策が不十分であるという現実が突きつけられました。特に顕著なのはVPNで、自宅や社外での勤務において欠かせない要素です。リモートワーカーをサポートするため、高品質、信頼性、俊敏性を実現できる、セキュアで高度な分散型ネットワークソリューションがこれまでになく求められています。Juniper® Session Smart™ SD-WANはゼロトラストファブリックを提供し、アプリケーションのパフォーマンスとトラフィック要件にシームレスに適応するルーティングにより、リモートワーカーが必要とする重要なリソースを管理し、アクセスを提供します。

課題

リモートワーク環境に対する需要が高まる中、世界中のエンタープライズのIT部門は、VPNサービスの可用性とセキュリティを重視するようになりました。VPNは通常、セキュリティ上の理由から、すべてのトラフィックをトンネルを介して企業ネットワークにルーティングします。これには、セキュアなパブリックSaaS (Software as a Service) アプリケーション (Microsoft Teams、Salesforce、Google Suitesなど)、標準のインターネットアクセス、顧客施設でホストされるサービスがあります。

従来、VPNソリューションはIPsecまたはSSLトンネリング技術を基盤としていました。このようなタイプのVPNは複雑で拡張が困難で、アプリケーションの制御や可視化に対応していません。企業がクラウドを導入し、IoT (モノのインターネット) が拡大し、モバイルユーザーが増加し、アプリケーションの応答性の向上が求められる中で、このようなトンネリング技術を利用した柔軟性に欠けるルーティングモデルはリモートワークの実現を難しくしています。このため、多くの企業がVPN/WANの高い費用に不満を抱き、これらのサービスの更新を検討しています。同時にネットワークを変革することで、企業はWANへの投資を最大化できます。

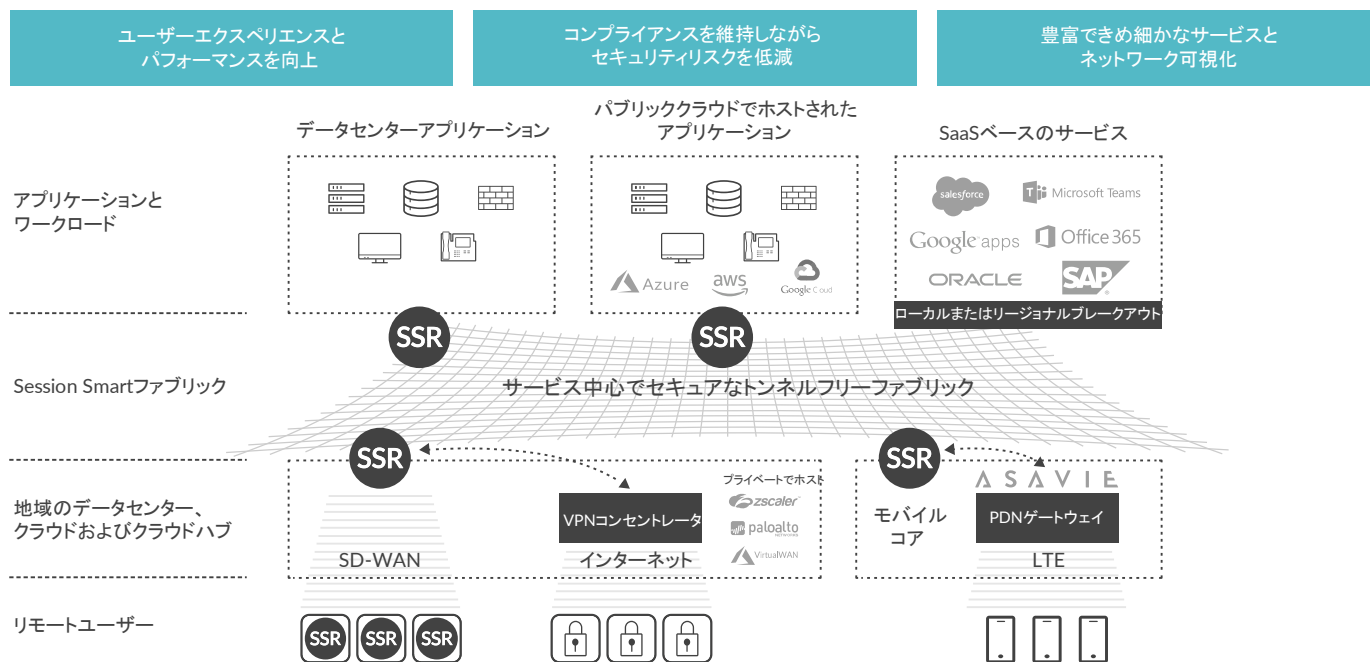


図 1: リモートユーザー向けSession Smart SD-WAN

Juniper Session Smart SD-WANソリューション

これまで、私たちの暮らしや生活においてネットワークの重要性をこれほど痛感することはありませんでした。実際に、セキュアで高度な分散型ネットワークソリューションのニーズはこれまでになく高まっています。Juniper Session Smart SD-WANソリューションによるサービス中心のファブリックで、「どこにいても働ける」アーキテクチャを簡素化し、俊敏性、セキュリティ、高品質のユーザーエクスペリエンスを独自に実現できます。

このソリューションの重要な機能として、Juniper Session Smart ルーターがアプリケーションのパフォーマンスニーズにダイナミックに適応し、それによってトラフィックをルーティングします。このトンネルフリーアプローチにより、アプリケーションの遅延を減らし、ビデオやその他のネットワーク負荷の高いアプリケーションで使用できる帯域幅を増やすことができます。ネイティブセッションの最適化を使用して、アプリケーションの速度と信頼性、品質、セキュリティ、コンプライアンスを向上できます。

今日の高度な分散型の「どこにいても働ける」環境は、セキュリティをネットワーク内に組み込む必要があり、従来の境界をベースとしたセキュリティアプローチとは相容れないものです。Session Smart SD-WANはゼロトラストファブリックを提供し、ユーザーが必要とする重要なリソースとデータへのアクセスを制御し、適切な場所に適切なタイミングでルーティングします。

Session Smartルーターのメリット

Juniper Session Smartルーターによって非効率なVPNトンネルが不要になり、一時的なセッションを有効化されるアプリケーションおよびサービスと関連付けることで、ネットワークをコンテキストに基づき認識できるようになります。この技術によって、一元管理、きめ細かな制御、個別化されたフロー、機能統合を実現し、このすべてにセキュリティとダイナミックなトラフィック管理を組み込むことで、リモートワーカーのニーズを企業がサポートする方法を簡素化できます。Session Smart SD-WANソリューションに組み込まれたインテリジェントな機能が、優れた品質、信頼性、拡張性をアプリケーションとサービスを提供し、リモートワーカーの利用が大幅に増えてもビジネスを継続できるよう、企業をサポートします。

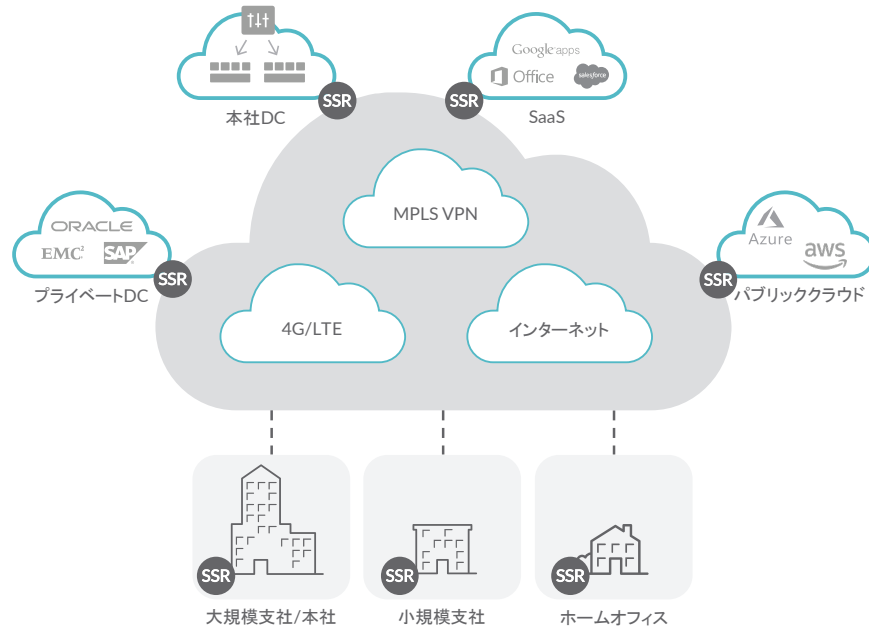


図2: Session Smart SD-WAN、トンネルフリーの接続性

Session Smart SD-WANソリューションにより、オーバーレイやトンネルが不要になるほか、サービス、テナント、ポリシー情報を一元化できます。これにより、自動化ツールが不要になり、複雑さが軽減され、可視化が向上し、最大限コストを削減できます。

さらに、このコンテキスト認識型のアプローチにより、予期しない問題が発生し、リモートワーカーをサポートする必要がある場合でも、企業のニーズのサポートを改善し、成功に向けて支援します。



図3: Session Smart SD-WANはコンテキスト認識型

特長とメリット

アプリケーション認識型ルーティング

IT部門は、アプリケーション認識型ルーティングを提供することで、ネットワークのパフォーマンスを改善できます。たとえば、Session SmartルーターはMicrosoft Office 365、Google Suitesなどのアプリケーションやその他のSaaSサービスを認識して、そのトラフィックをWANに直接オフロードします。企業でホストされたアプリケーションのみがデータセンターにルーティングされます。さらに、ダイナミックセッションとアプリケーション認識により、セッションポリシーとネットワークのステータスに基づいてロードバランシングとトラフィックステアリングを提供します。この機能は、数百名の従業員が急遽オフサイトで働くことになった場合に不可欠です。

FIPS 140-2認定

米国政府のコンピュータセキュリティに関する規格FIPS-140-2は、暗号化モジュールを承認し、機密性を保持するために使用されます。Session Smart SD-WANはこの認定要件を満たし、企業はPCI (Payment Card Industry) およびHIPAA (医療保険の携行と責任に関する法律) の要件に準拠するネットワークを構築できます。さらに、Session SmartルーターはICSA Labs Network Firewall認定を受け、PCI認証を達成しています。従業員が働く場所がどこであっても、企業はネットワークとデータの安全性を保証できます。



図4:FIPS-140-2およびICSA Labs Network Firewall認定

ゼロトラストセキュリティ

Session Smart SD-WANを使用すると、企業はゼロトラストセキュリティをベースにネットワークを構築でき、関連付けられたセキュリティポリシーに基づき、各フローが確実に暗号化して認証されます。このため、企業の管理者は、従業員が自宅で働いているときでも、マイクロセグメント化された接続または個別化されたVPNを、大規模組織内のさまざまな事業部門に安全に提供できます。



図5:Session Smart SD-WANソリューションの機能

可視化の強化

Juniper Session Smart Conductorは、分散型Session Smartルーターに、一元化されたオーケストレーション、管理、ゼロタッチプロビジョニング、監視、分析を提供します。これらのツールは、ネットワーク全体の統一された表示と強化されたセッション統計を提供するため、リモートワーク環境における重要性が高まっています。これを利用して管理者は、選択したKPI (主要パフォーマンス指標) に基づいてカスタマイズしたチャートや、セキュリティとトラフィックのイベントに関する詳細レポートを生成できます。これにより、従業員が分散していても、企業のコンプライアンス要件を満たしながら、ネットワーク攻撃を検出して防止できます。



Session Smart SD-WANのユースケース

自宅でのSession Smart SD-WAN

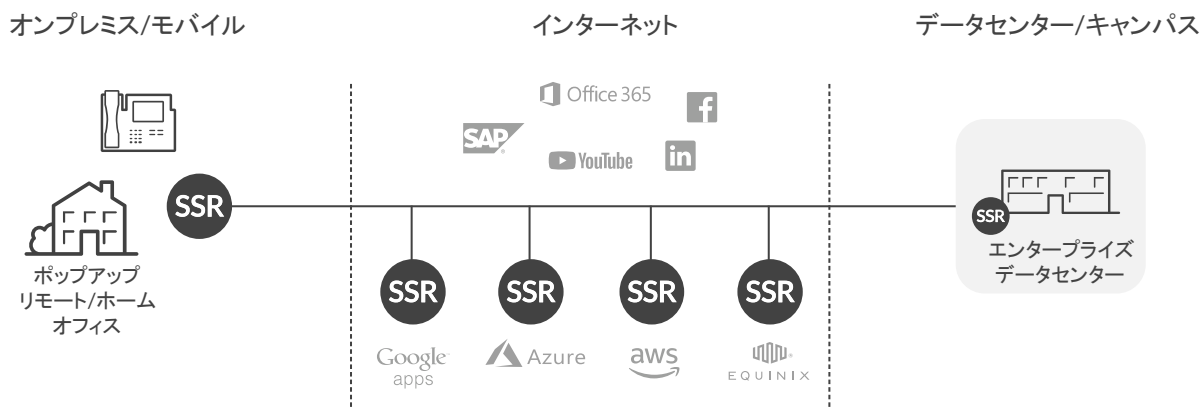


図6. 自宅でのSession Smart SD-WAN

お客様のメリット

ユーザーエクスペリエンス	セキュリティとコンプライアンス	可視化
<ul style="list-style-type: none"> • アプライアンスへのシンプルな接続 • 低遅延と高スループット • ゼロタッチプロビジョニング 	<ul style="list-style-type: none"> • FIPS 140-2 • インサイドアウト接続 • マイクロセグメント化されたアクセス 	<ul style="list-style-type: none"> • セッションごとの監査 • テナントおよびサービスのパフォーマンス • 完全に分散された分析

このユースケースでは、1つのSession Smartルーターが自宅に導入され、もう1つがデータセンターまたはクラウドに導入されています。アプリケーションは宛先に応じてインテリジェントにルーティングされます。たとえばSaaSアプリケーションがWANに直接オフロードされる場合、高度なUTM (Unified Threat Management) 処理を必要とするエンタープライズアプリケーションをエンタープライズデータセンターにルーティングできます。

クラウドでのSession Smart SD-WAN



図 7: クラウドでのSession Smart SD-WAN

お客様のメリット

ユーザーエクスペリエンス	セキュリティとコンプライアンス	可視化
<ul style="list-style-type: none"> VPNクライアントエクスペリエンス (ポータル/ログイン) クラウドベースのスケーリング シームレスな接続 	<ul style="list-style-type: none"> FIPS 140-2 インサイドアウト接続 マイクロセグメント化されたアクセス 	<ul style="list-style-type: none"> セッションごとの監査 テナントおよびサービスのパフォーマンス 完全に分散された分析

このユースケースでは、リモートワーカーは標準的な技術を使用してクラウドのVPNゲートウェイに接続します。するとトラフィックはSession Smartルーターに引き渡され、パケットは正しい宛先にインテリジェントにルーティングされます。Session Smartルーターは、企業ネットワークにルーティングされるRFC1918ネットワークと、その他すべてのトラフィック (サービスに直接ルーティングされる、またはUTMソリューションを通じてルーティングされるクラウドサービスを含む) を区別できます。

プライベートLTEアクセスのあるデータセンターでの Session Smart SD-WAN

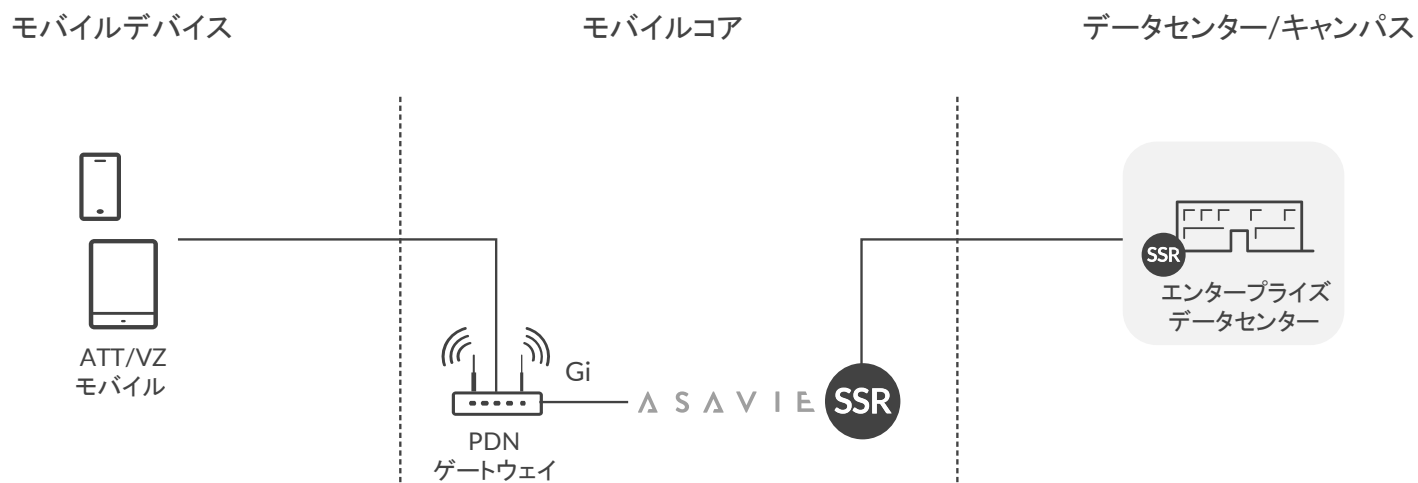


図 8: プライベートLTEアクセスのあるデータセンターでのSession Smart SD-WAN

お客様のメリット

ユーザーエクスペリエンス	セキュリティとコンプライアンス	可視化
<ul style="list-style-type: none"> クライアントベースのエクスペリエンス (ポータル/ログイン) クラウドベースのスケーリング シームレスな接続 	<ul style="list-style-type: none"> FIPS 140-2 インサイドアウト接続 マイクロセグメント化されたアクセス 	<ul style="list-style-type: none"> セッションごとの監査 テナントおよびサービスのパフォーマンス 完全に分散された分析

このユースケースでは、Asavieとのパートナーシップを利用してエンドツーエンドのセキュアプライベートLTE接続を提供し、リモートワーカーの接続をサポートしています。Session Smart SD-WANはLTEコアおよびエンタープライズデータセンターに導入され、ネットワークセキュリティ、ネットワークアクセス制御、アプリケーション認識型ルーティング、コンプライアンスを実現します。

Session Smart SD-WANとWireguard

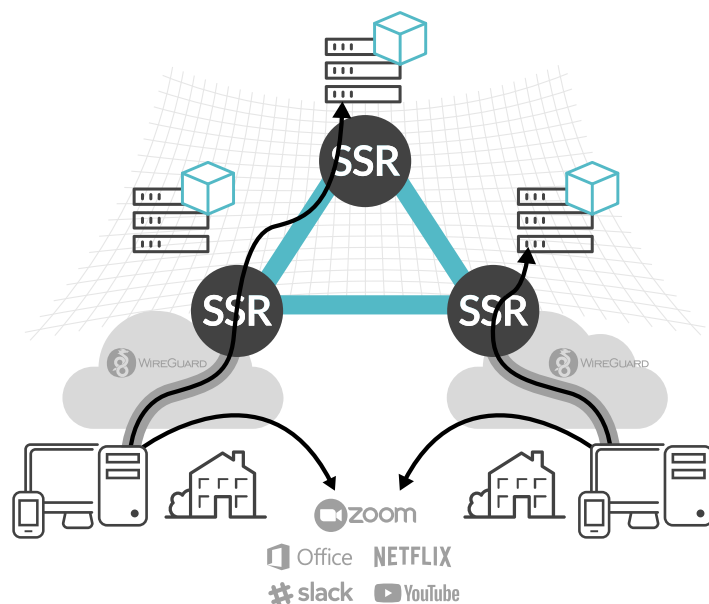


図 9: Session Smart SD-WANとWireguard

お客様のメリット

ユーザーエクスペリエンス	セキュリティとコンプライアンス	可視化
<ul style="list-style-type: none"> ゼロタッチエクスペリエンス (Wi-Fi接続) クラウドベースのスケーリング ゼロタッチプロビジョニング 	<ul style="list-style-type: none"> FIPS 140-2 インサイドアウト接続 マイクロセグメント化されたアクセス 	<ul style="list-style-type: none"> セッションごとの監査 テナントおよびサービスのパフォーマンス 完全に分散された分析

こちらの最後の導入ケースでは、オフィス外で使用するために設計された企業のデバイスを、無料のオープンソースVPNソリューションである軽量のWireguardで設定し、企業のトポロジーの1つ（または複数）のSession Smartルーターとピアリングさせます。選択的かつインテリジェントに、セキュアなセッションを、サービスがアクセスできるSession Smartルーターのピアに送信し、セキュアなSaaSおよびコンシューマサービスをブロードバンドに直接オフロードします。WireguardをSession Smartルーターと組み合わせて、社内ネットワークアクセスエッジをオフィス外のユーザーに拡張できます。

まとめ - Session Smart SD-WANで リモートワーカーの設定を成功に導く

ジュニパーのSession Smart SD-WANソリューションは、制御の一元化、コンテキスト認識型ネットワークの導入の簡素化、インバンドシグナリングによるインテリジェントなサービスルーティング、きめ細かなマイクロセグメンテーション、ゼロトラストモデルに基づく組み込みセキュリティを提供します。これらの機能と能力を組み合わせることで、従来のルーター製品の機能をはるかに上回り、リモートワークの成功を阻む根本的なネットワークの問題を解決します。

その結果が、ダイナミックかつセキュアに境界を越えて容易に拡張できるコンテキスト認識型ネットワークで、組織はアプリケーションに対応しやすいインフラストラクチャを構築して、分散して働く従業員のニーズにも柔軟に対処できます。

次のステップ

Session Smart SD-WANがリモートワーカーをサポートする方法の詳細については、ジュニパーアカウントマネージャーにお問い合わせいただくか、www.juniper.netをご覧ください。

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、世界をつなぐ製品、ソリューション、サービスを通じて、ネットワークを簡素化します。エンジニアリングのイノベーションにより、クラウド時代のネットワークの制約や複雑さを解消し、お客様とパートナー様の日々直面する困難な課題を解決します。ジュニパーネットワークスは、世界に変革をもたらす知識の共有や人類の進歩のリソースとなるのはネットワークであると考えています。私たちは、ビジネスニーズにあわせた、拡張性の高い、自動化されたセキュアなネットワークを提供するための革新的な方法の創造に取り組んでいます。

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

アジア太平洋地域、 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: +31.0.207.125.700
FAX: +31.0.207.125.701

日本

東京本社
ジュニパーネットワークス株式会社
〒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
www.juniper.net/jp

JUNIPER | Engineering
NETWORKS® | Simplicity