

GOOGLE CLOUD PLATFORM 向け vSRX 仮想ファイアウォール

製品概要

vSRX 仮想ファイアウォール は、サービスプロバイダや企業向けに、高度なセキュリティ、セキュアな SD-WAN、堅牢なネットワーキング、自動化された仮想マシンのライフサイクル管理を含めた、Google Cloud Platform 向けの完全なクラウドネイティブ仮想ファイアウォールを提供します。Google Cloud Platform 向け vSRX のトライアル版をアクティベートする場合は、[GCP マーケットプレイス](#)をご覧ください。

製品説明

ワークロードがパブリッククラウドに移行すると、クラウドと他の場所で実行されているワークロード間のデータと通信のセキュリティに関連した問題が生じます。

ネットワーク専門家やセキュリティ専門家は、企業のセキュリティを弱体化させることなくクラウド技術のメリットを享受できるように、微妙なバランスを取る必要に迫られます。進化する脅威に対応しながら、信頼性、可視性、制御性を損なわずにクラウド環境の俊敏性と拡張性についていけるリユースのみが、この課題に応えられます。

ジュニパーネットワークスは、受賞歴のある [ジュニパーネットワークス®SRX シリーズvSRX 仮想ファイアウォール](#)の機能を Google Cloud Platform (GCP) 向けのクラウドネイティブな仮想ファイアウォールとして拡張し、セキュリティ専門家が GCP 内で実行するワークロードにファイアウォール保護を導入し拡張できるようにすることで、こうした課題に真っ向から取り組んでいます。ジュニパーネットワークスの vSRX 仮想ファイアウォールは、侵入防御システム (IPS)、マルウェア防御、アプリ制御、オンデマンド脅威検知などが含まれる、比類のない [次世代ファイアウォール \(NGFW\)](#) セキュリティを提供します。また、vSRX は、SD-WAN、GCP 仮想ネットワーク、SD-LAN とのセキュアな通信をサポートし、ワークロード間のセキュアなセグメント化も確保します。

ネットワークおよびセキュリティ管理者は、クラウド環境の変化するニーズに応じて、GCP 向け vSRX の自動プロビジョニング機能を活用することで、ファイアウォール保護メカニズムを迅速かつ効率的に導入して拡張できます。管理者は、vSRX を [Junos Space® Security Director](#) または Contrail® サービスオーケストレーションの機能と組み合わせることで、一元化された汎用プラットフォームからポリシーの設定、管理、および物理的資産と仮想資産の両方の可視性を大幅に向上させることができます。

ジュニパーは、お客様が既存の投資価値を実現できるようサポートし、SRX シリーズのすべてのファイアウォールで相互運用性を確保するために尽力しています。vSRX は、Security Director と Contrail Service Orchestration に加えて、OpenContrail やその他のサードパーティによる管理ソリューションもサポートしています。また、vSRX は、OpenStack などの他の次世代クラウドオーケストレーションツールとも、直接または豊富な API を通じて統合することができます。

パブリッククラウドや従来の仮想化のユースケースに加えて、vSRX ではサービスプロバイダおよび企業が、エッジ防御機能を備えた安全な SD-WAN ファブリックを導入することが可能です。セキュアな SD-WAN ファブリックは、あらゆるサイトの個別ニーズに適応すると同時に、ネットワーク上のどこに仮想化アプリケーションやサービス重視のアプリケーションが存在するのであれ防御できる柔軟性を備えています。

Security Director は、物理、仮想またはコンテナを問わず、最大 25,000 台の SRX シリーズファイアウォールを単一の管理インスタンスから管理できます。このツールにより、企業は、エンドポイントからエッジ、そしてその間にあるすべてのクラウドにいたるまで、単一のプラットフォームから、ネットワークセキュリティ、仮想化、相互接続を管理、自動化、オーケストレーションすることができます。

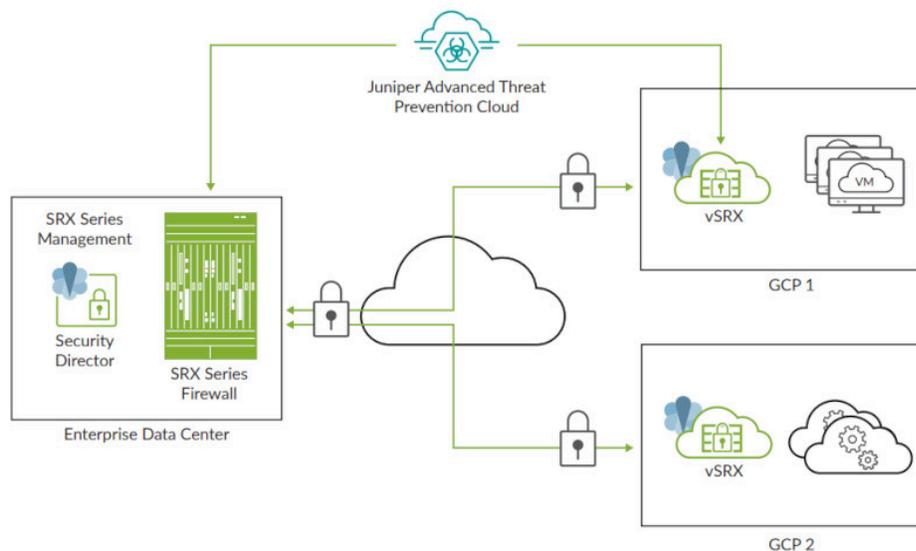


図1 : GCP でワークロードを保護する vSRX

アーキテクチャと主要コンポーネント

セキュアな接続性

GCP 上の vSRX は、異なる仮想ネットワークやオンプレミスデータセンターで稼働するワークロード間の通信を保護することができます。vSRX の VPN 機能により、同じ GCP リージョン内の仮想ネットワーク同士のピアリングや、GCP リージョン全体のグローバルな仮想ネットワークピアリングを安全に接続することができます。VPN 機能により、vSRX は、データフローをインターネット経由で送信することなく、GCP 仮想ネットワーク間の安全な接続を実現できるため、コスト、遅延および可用性上の懸念を最小限に抑えることができます。

また、vSRX 仮想ファイアウォールでは、複数の接続オプションを使用して、サイトを安全に接続することもできます。エンタープライズ WAN ファブリックに対する仮想または物理のどちらの接続であれ、他のデータセンター（サードパーティクラウド展開のコロケーションなど）にまで安全な接続性を拡張することで、クラウドのワークロードと通信する必要が生じることがあります。

セキュアな SD-WAN

Google Cloud でホストされているアプリケーションにアクセスするにあたり、従来の支社/拠点では、企業のキャンパス拠点を經由して GCP アプリケーションにアクセスする接続を利用していました。このような状況では、支社/拠点にセキュアな SD-WAN を導入し、GCP 上で vSRX を使用することで、キャンパスネットワーク経由でクラウドアプリケーションにアクセスする必要性を回避し、GCP に直接接続できるより最適なソリューションを実現できます。

GCP に導入された vSRX は、SD-WAN のスポークまたはハブとして機能し、より大規模な SD-WAN 導入の一環として、キャンパスや支社/拠点と GCP 間の安全なアクセスを直接サポートすることができます。また、SD-WAN ハブとして機能することで、GCP にホストされているクラウドリソースへの安全なアクセスを提供することもでき、地域ベースのインターネットブレイクアウトの中央点となることもできます。この中央点により、GCP 上の vSRX がワークロードを保護し、変化するビジネスニーズに適応する安全な SD-WAN 接続を提供することができます。

ワークロードの保護

ファイアウォールはワークロードを保護しますが、すべてのファイアウォールが同じように作られるわけではありません。GCP 上の vSRX を利用することで、お客様はワークロードがオンプレミス、パブリッククラウド、エッジのいずれで稼働しているのであれ、ネットワーク全体で一貫したポリシーを展開できるようになります。すでに SRX シリーズファイアウォールをネットワーク上で活用されているお客様は、パブリッククラウドなどで運用されている vSRX 仮想ファイアウォールへとポリシーを簡単に拡張することができます。

vSRX は、メタデータタグを使用したファイアウォールポリシーの作成と展開をサポートしており、セキュリティの自動化を促進し、初期導入時や継続的なメンテナンス時に必要となるルール数を削減します。このメタデータは、セキュリティ管理者にメタデータタグに基づくネットワークの全体ビューを提供して、可視化を向上させます。つまり、IP アドレススペースのルール管理とフィルタリングに制限されなくなります。

vSRX はポリシーを適用するだけでなく、IPS、アンチウイルス、アンチマルウェアなどの高度なセキュリティサービスも提供して

おり、GCP クラウドでホストされているワークロードを標的とした高度な脅威を特定してブロックします。

ワークロードのセグメント化

vSRX は、ワークロードセグメント間で許可される通信に関するポリシーを適用することで、GCP 上の通信を保護し、ワークロードのセグメント化を確保することができます。vSRX により、仮想化されたワークロードレベルでセキュリティポリシーを適用できるため、きめ細かいネットワークのセグメント化と制御が容易になります。セキュリティの観点からは、脅威をブロックする粒度の細かさが細かいほど、脅威の伝播を効果的に封じ込めることができます。

特長とメリット

高度なセキュリティ サービス

従来のファイアウォールや個々のスタンドアロンアプライアンスやソフトウェアを中心に構築された、統合されていないレガシーシステムを導入しても、今日の高度な攻撃から保護するには十分ではありません。

ジュニパーの高度なセキュリティパッケージでは、ユーザーが現代の組織による進化する個別のニーズや常に変化する脅威に合わせて複数の技術を導入できます。技術やポリシーなどのセキュリティ機能はリアルタイムで更新され、常に最新の状態で保たれます。

GCP 向け vSRX は、IPS、マルウェア防御、アプリケーション制御、コンテンツセキュリティなど、汎用性があり強力な高度なセキュリティサービスを提供します。

侵入防御システム

GCP 用 vSRX の IPS は、IT ネットワークへのアクセスを制御し、データを検査し、攻撃が発生した際にブロックしたり、ファイアウォールに一連のルールを作成するなどのアクションを起こすことで、システムを保護します。IPS はジュニパーのアプリケーションセキュリティ機能とネットワークインフラストラクチャを密接に統合させることで、脅威を緩和してさまざまな攻撃や脆弱性を阻止します。

Juniper Advanced Threat Prevention

[Juniper® Advanced Threat Prevention](#) を GCP 向け vSRX と統合することで、既知のマルウェアや高度なゼロデイ脅威に対する動的な自動保護が提供され、ほぼ瞬時に対応できるようになります。

AppSecure によるアプリケーションの可視化と制御

ジュニパーネットワークスの AppSecure は、脅威の可視化、保護、ポリシー適用、制御を実現する、次世代型アプリケーション

セキュリティスイートです。このオプション機能が、強力な可視化と継続的なアプリケーション追跡を提供します。オープンシグネチャを使って独自のアプリケーションセットを監視し、計測し、コントロールすることで、組織のビジネス上の優先度に基づいてアプリケーションを適切に使用できます。

コンテンツセキュリティ

GCP 向け vSRX は、マルウェア、ウイルス、フィッシング攻撃、スパムなどの脅威に対抗する非常に優れたアンチウイルス、アンチスパム、Web フィルタリング、コンテンツフィルタリングが含まれる包括的なコンテンツセキュリティ機能を提供します。

Juniper Secure Connect

[Juniper Secure Connect](#) は、柔軟性に優れた SSL VPN アプリケーションであり、保護されたリソースから離れた場所で業務に取り組む従業員に、企業やクラウドリソースへのセキュアなアクセスを提供します。この SSL VPN アプリは、ほとんどの一般的なオペレーティングシステムで利用できます。あらゆる場所のすべてのデバイスに適應可能な接続性を提供し、ユーザーからクラウドまで可視性と適応力を拡張することでリスクを低減します。

表 1. GCP 向け vSRX の特長とメリット

特長	説明	メリット
拡張可能なハードウェアサポート	2つのCPUコアと7.5GBのメモリで始めて、最大16コアと60GBのメモリにまで拡張することが可能	トラフィックの増加に伴い、現在および将来のニーズをサポートする柔軟で拡張性のあるハードウェアフットプリントを提供
柔軟なライセンス	従量制 (PAYG) オプションと利用者所有ライセンス (BYOL) オプションの両方をサポート	GCP 内のワークロードを保護し、データセンターと GCP 間の接続性を確保する柔軟なライセンスと購入オプションを提供

仕様

表 2. GCP 上 vSRX のインスタンスタイプ

GCP インスタンスタイプ	インスタンスタイプの vCPU	インスタンスタイプのメモリ (GB)
N1-standard-2	2	7.5
N1-standard-4	4	15
N1-standard-8	8	30
N1-standard-16	16	60

サポートされている GCP インスタンスタイプの全リストについては、www.juniper.net/documentation/ja_JP/vsrx/topic/topic-map/security-vsrx-google-system-requirements.html を参照してください。

注文情報

ジュニパーネットワークスの GCP 向け vSRX 仮想ファイアウォール BYOL の詳細な情報については、www.juniper.net/jp/ja/products-services/security/srx-series/vsrx をご覧いただくか、ジュニパーネットワークス営業担当者までお問い合わせください。

GCP 向け vSRX のトライアルバージョンを有効にされる場合は、GCP マーケットプレイス (<https://console.cloud.google.com/marketplace/details/juniper-marketplace/vsrx-next-generation-firewall?q=vsrx&id=de0a15a3-968e-4bed-8eca-e892b06e8701>) をご覧ください。

製品	説明
vSRX 仮想ファイアウォール	<ul style="list-style-type: none"> IPsec VPN、ネットワークアドレス変換 (NAT)、サービスコスト、豊富なルーティングサービスを備えたコアファイアウォール AppID、AppFW、AppQoS、AppTrack を備えた AppSecure IPS などのコンテンツセキュリティサービス
アンチウイルス保護を備えた vSRX 仮想ファイアウォール	<ul style="list-style-type: none"> コアファイアウォール機能、IPsec VPN、NAT、サービスコスト、豊富なルーティングサービス AppID、AppFW、AppQoS、AppTrack を備えた AppSecure IPS、アンチウイルス、アンチスパム、Web、コンテンツフィルタリングを含むコンテンツセキュリティサービス

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、ネットワークを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。

Corporate and Sales Headquarters

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

www.juniper.net

APAC and EMEA Headquarters

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

www.juniper.net/jp/ja/

