Cloud Secure Edge

リモートアクセス、より優れたセキュリティ

SonicWall Cloud Secure Edge™は、非常に効果が高く導入が簡単なセキュリティサービスエッジ（SSE）ソリューションであり、ワークフォースがあらゆるデバイスからあらゆるリソースへ安全にアクセスすることを可能にします。ネットワークの場所を問わず、プライベートリソースとインターネットリソースへのシンプルで安全なゼロトラストアクセスをすべての従業員とサードパーティに提供します。また、複数の従来型ネットワークアプライアンス（リモートアクセスVPN、ウェブプロキシ、ファイアウォールなど）の機能を統合クラウド型ソリューションに集約し、ワークフォース全体のセキュリティ体制とユーザーエクスペリエンスを向上させます。

注意：SonicWall Gen 7ファイアウォールを導入済みのお客様は、Cloud Secure Edgeにすぐに接続して、統合されたダッシュボードからアクセスポリシーを管理できます。

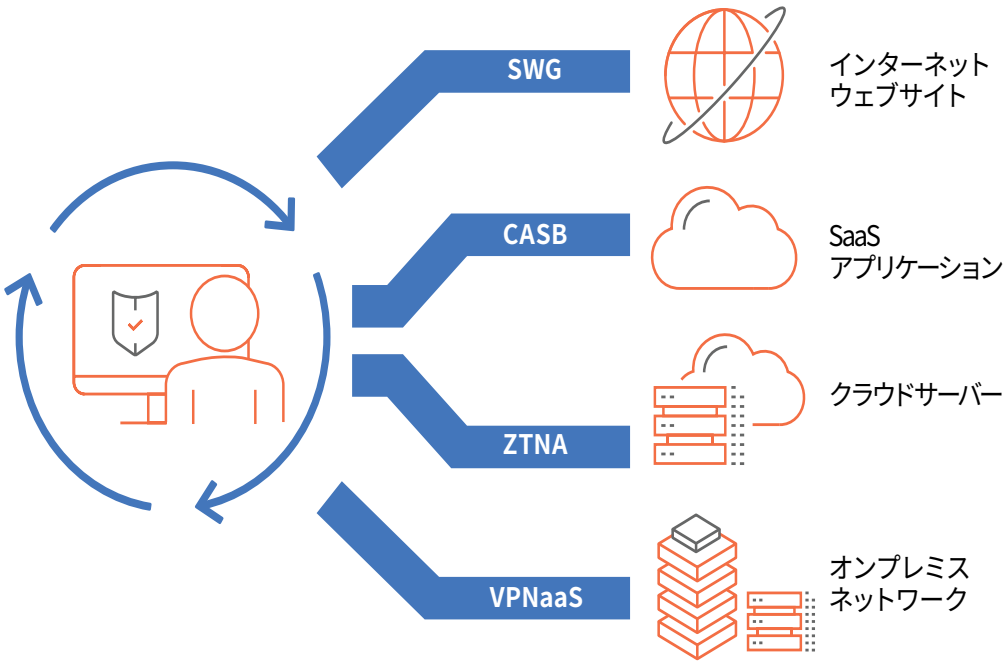

図1：あらゆるデバイスからあらゆるリソースへのアクセスを保護するSonicWall Cloud Secure Edge

データシート

SonicWall Cloud Secure Edgeを選ぶ理由

導入と管理が簡単

Cloud Secure Edgeは、スタンドアロンとして、または既存のSonicWall Gen 7ファイアウォールに追加して、月額サブスクリプションで使用できます。 低TCOや短期間でのROI回収を求めているMSPおよびリソースが過度に膨張しているDIY組織に最適です。

最新の脅威に対する防御

Cloud Secure Edgeにはゼロトラストセキュリティ制御機能があります。これは、あらゆる場所から仕事ができるようにするために必要な機密性の高いプライベート資産やインターネット資産にアクセスする必要があるハイブリッドワークフォースやリモートワークフォースにとって欠かせないものです。デバイス中心およびID中心の信頼スコアリングと有効期間の短い暗号化をベースとした独自のテクノロジーを採用しており、卓越したユーザーエクスペリエンスを備えた、業界をリードするセキュリティを提供します。

パフォーマンスとプライバシーの両立

Cloud Secure Edgeは、プライバシーの確保と高いパフォーマンスの実現を両立するためにゼロから構築されました。管理者はデータを完全に制御しつつ、最大限の生産性、データ保護、プライバシーのための可能な限り自然かつ効率的な接続をユーザーに保証します。

一般的なユースケース

ZTNAを用いたVPNとファイアウォールのモダナイゼーション

Cloud Secure Edgeは、ファイアウォールやレガシーVPNのような大まかなツールで企業のリソースを保護するのではなく、ユーザーやデバイスの信頼性とリソースの機密性というリアルタイムのコンテキストの要因の組み合わせに基づき、特定のアプリケーションやサーバーに最小権限でアクセスすることを可能にします。

Cloud Secure Edgeはクラウドベースであり、単独で、または既存のセキュリティインフラストラクチャと組み合わせて適用できます。

インターネット上の脅威や認証情報の侵害からの保護

SonicWallは高性能のグローバルエッジPOPを導入し、最も効率的でダイレクトなルーティングを確保しながら、一貫した適用制御によってあらゆる種類の攻撃やリスクの高い露出から保護します。これにより、フィッシング攻撃や悪意のあるウェブサイトに対してシンプルで効果的な保護を提供すると同時に、必要に応じてコンテンツフィルタリングを適用し、アクセスが許可される前に適切な方法でデバイスのセキュリティが事前に検証されます。

リスクの高いユーザー（サードパーティ/ BYOD / M&A）の保護

サードパーティに対して、過剰なプロビジョニングを行うことなく、必要な特定のリソースのみへの簡単かつ安全なアクセスを提供します。Cloud Secure Edgeは、ユーザーとデバイスのセキュリティ体制だけでなく、ユーザーの役割やユーザーが閲覧を認められているものにも基づいてアクセスを保証します。管理は、グループと役割を事前に識別して1つの集中管理コンソールから必要に応じて適用できるため、簡単です。パッチの適用やハードウェアの設定は不要です。

ライセンス

Cloud Secure Edgeは、（内部ネットワーク上のリソースへの）Secure Private Accessおよび（パブリックインターネット上のリソースへの）Secure Internet Accessとして利用できます。

1. Secure Private Accessには、次の2つのコア機能があります。
   - トンネルベースZTNA（Cloud VPNまたはVPNaaSとも呼ばれます）：特定のネットワークセグメントへの安全なネットワークアクセス。
   - プロキシベースZTNA：社内のHTTPアプリケーションやTCPサービスなどのプライベートリソースへの安全なアクセス。
2. Secure Internet Accessには、次の3つのコア機能があります。
   - DNSレイヤーセキュリティ（DNS）：ドメインレベルの脅威保護：悪意のあるドメインのブロックや利用規約の適用。
   - クラウドアクセスセキュリティブローカー（CASB）：SaaSアプリケーションにアクセスするためのデバイス信頼ポリシーを適用。
   - セキュアウェブゲートウェイ（SWG）：暗号化されたウェブトラフィック内に潜んでいるマルウェアやその他の脅威をブロックするためのウェブコンテンツフィルタリング。

Secure Private Access（SPA）のSKUとSecure Internet Access（SIA）のSKUは、どちらもBasicおよびAdvancedの2つのティアで利用できます。ライセンスはユーザー単位で販売されます。

共通機能

高性能なデータプレーン

世界中のユーザーに高速で
信頼性の高い接続を提供するための
ダイナミックなエッジアーキテクチャ

すべてのクライアントオペレーティングシステムをネイティブにサポート

デスクトップ（Windows、macOS、Linux）
およびモバイル（iOS、Android、ChromeOS）

クラウド管理インターフェイス

ゼロトラスト接続を設定するIT管理者や
セキュリティ管理者向け

信頼スコアリング

ユーザーやデバイスに関連する
信頼性とリスクのレベルを数値化

実用的な可視性

ユーザー/デバイスおよび
アプリケーション/リソースのリスクを
完全に可視化

継続的なポリシー適用

ユーザーの場所に関係なく、
リソースの機密性がベース

統合機能

既存のツール（IDP、EDR、MDM、SIEM）
との統合

SonicWallファイアウォールコネクター

7.1.2以降のグローバルモードですぐに使用
できるGen7ファイアウォールとの統合

マルチテナント管理

マルチテナント管理のための
クラウドベースのポリシー

ユーザーおよびデバイス

シングルサインオン

ジャストインタイム（JIT）ユーザー作成で
企業のシングルサインオンを使用

ポスチャ管理

ファイアウォール、ディスク暗号化、
画面ロック、OSバージョンなど、
デバイスのポスチャを分析

信頼プロファイル

ユーザーとデバイスのグループに基づいて
要素とポリシーの効果をカスタマイズ

カスタム修復

エンドユーザーに対して表示される
メッセージングやリンクなどの
デバイスポスチャ修復手順を設定

可視性およびコンプライアンス

リアルタイムのイベントストリーム

ユーザーとデバイスのアクティビティの
リアルタイムストリームを監視

デバイスポスチャレポート

企業のリソースにアクセスするすべての
デバイス（管理対象および非管理対象）と
それぞれのセキュリティ体制を追跡

管理者アクティビティレポート

すべての管理アクティビティのログを
Cloud Command Centerに記録

運用および自動化

RESTful API

コントロールプレーンでCSEオブジェクトを
設定するためのRESTfulエンドポイント

APIクライアント – pybanyan、Terraform

自動化と管理のための
PythonライブラリとTerraform

ゼロタッチデバイスデバイス登録

エンドユーザーの操作を必要とせずに
CSEアプリをデバイスフリートに展開

	Secure Private Access		Secure Internet Access	
特徴	Basic	Advanced	Basic	Advanced
安全なネットワークアクセス				
ZTNAトンネル（VPNaaS）による、特定のネットワークへのアクセス	✓	✓		
ZTNAプロキシによる、社内のHTTPアプリケーションやTCPサービスへの安全な接続		✓		
プライベートネットワーク（RFC-1918の範囲）およびドメイン（社内DNSサーバー）	✓	✓		
特定のサブネットやドメイン（プライベートまたはパブリック）へのスプリットトンネリング	✓	✓		
すべてのトラフィックに対するフルトンネリング		✓		
CIDRおよびFQDNに基づくネットワーク/レイヤー4ポリシー	✓	✓		
プライベートリソースへの安全なアクセス				
ブラウザのみのOpenID Connectフローを用いた社内ウェブサイトへのアクセス		✓		
SSHによるLinuxサーバーへの接続		✓		
RDPによるWindowsマシンへの接続		✓		
PostgreSQLやMySQLなどのデータベースサーバーにアクセスするためのネイティブクライアント		✓		
クラスターにアクセスするためのKubernetesクライアント		✓		
SSH証明書認証、プリンシパルの承認、監査ログ		✓		
API、ウェブページにアクセスするためのレイヤー7ポリシー		✓		
インターネット上の脅威からの保護				
マルウェア、フィッシング、ボットネット、その他のリスクが含まれているドメインをブロックするDNSレイヤーセキュリティ			✓	✓
コンテンツの分類			✓	✓
カスタムブロッキング			✓	✓
SaaSアプリケーションのセキュリティ				
クラウドアクセスセキュリティブローカー（CASB）による、SaaSアプリケーションへのデバイス信頼ポリシーの適用				✓
クラウドアプリケーション/シャドーITの可視化				✓
SonicWall Edgeによるクラウドアプリケーションの IP許可リスト				✓
Okta向けDevice Trust				✓
Azure AD向けDevice Trust				✓
OneLogin、Jumpcloudなど、その他のIDP向けDevice Trust				✓
ウェブコンテンツフィルタリングサービス				
セキュアウェブゲートウェイ（SWG）：DNS経由のコンテンツフィルタリング			✓	✓
セキュアウェブゲートウェイ（SWG）：DNS経由の脅威フィルタリング			✓	✓
ユーザーおよびデバイス				
IDPフェデレーション経由のパスワードレス認証		✓		✓
信頼済みデバイス証明書による、未登録デバイスからポリシーを適用したアクセス		✓		✓
クライアントレスアクセス		✓		✓
サービスアカウント（データプレーンを通じたスクリプティングや自動化などのプログラムによるアクセスのためのAPIトークン）		✓		
ユーザー割り当てを管理するためのSCIM統合		✓		✓
EDR統合（CrowdStrike、SentinelOne、Microsoft Defenderなど）		✓		✓
MDM/UEM統合（JAMF、Kandji、Jumpcloud、Intune、Workspace Oneなど）		✓		✓

SONICWALL

可視性およびコンプライアンス				
SIEM統合（Splunk、Elastic、Sumo Logicなど）		✓		✓
プライベートネットワーク探索（ユーザーまたはデバイスによってアクセスされる承認されていないアプリケーション）		✓		該当なし
IaaSリソース探索		✓		該当なし
SaaSアプリケーション探索		該当なし		✓
運用および自動化				
プライベートエッジでの導入：SonicWallのID認識ゲートウェイを独自のインフラストラクチャでホスト		✓	該当なし	該当なし
サービスおよびサポート				
24時間365日のサポート	✓	✓	✓	✓
プレミアサポート		アドオン		アドオン
リモート導入サービス		アドオン		アドオン

まとめ

SonicWall Cloud Secure Edgeは、業界をリードするTCOとエンタープライズグレードのゼロトラストセキュリティを組み合わせたセキュリティサービスエッジソリューションです。物理的な場所やデバイスを問わず、プライベートリソースとインターネットリソースへのシンプルで安全なゼロトラストアクセスを従業員とサードパーティに提供します。Cloud Secure Edgeは複数の従来型ネットワークアプライアンス（リモートアクセスVPN、ウェブプロキシ、ファイアウォールなど）の機能をあらゆる規模の組織にとって導入がシンプルで管理しやすい統合クラウド型ソリューションに集約し、皆様と皆様の顧客のROIを最大化します。

SonicWall Cloud Secure Edgeの詳細はこちらをご覧ください。

Cloud Secure Edgeを既存のSonicWall Gen 7ファイアウォールに追加することをご希望の場合は、アカウントエグゼクティブにお問い合わせください。

SonicWallについて

SonicWallは、30年以上の実績を誇り、絶えずパートナー企業を重視しているサイバーセキュリティの先駆者です。クラウド、ハイブリッド、従来型ネットワークが混在する環境にリアルタイムでセキュリティを構築、拡張、管理するSonicWallは、世界中のあらゆる組織に専用のセキュリティソリューションを短時間で経済的に提供します。SonicWallは、自社の脅威研究センターのデータに基づいて、巧妙なサイバー攻撃に対するシームレスな保護を提供し、パートナー、お客様、サイバーセキュリティコミュニティに実用的な脅威インテリジェンスを提供します。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細は当社ウェブサイトをご覧ください。
www.sonicwall.com

© 2024 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWallは、SonicWall Inc.またはその関連会社の米国および他国における商標または登録商標です。その他すべての商標および登録商標は、それぞれの所有者に帰属します。本文書の情報は、SonicWall Inc.および/または関連会社の製品に関連して提供されています。本文書またはSonicWall製品の販売に関連しては、明示されているか否かにかかわらず、また禁反言によるとよらずにかかわらず、いかなる知的所有権のライセンスも許諾するものではありません。本製品の使用許諾契約書の定める契約条件で規定されている場合を除き、SonicWallおよび/またはその関連会社はいかなる責任を負うものではなく、また、製品に関するいかなる明示的、黙示的、もしくは法定上の保証（商品性、特定目的への適合性、非侵害性に関する黙示的な保証を含むが、これに限定されない）についても一切の責任を負わないものとします。SonicWallおよび/またはその提携会社は、本文書の使用または不使用に起因して発生した、いかなる直接的、間接的、派生的、懲罰的、特殊、または偶発的な損害（利益の損失、営業停止、情報消失を含む）について一切責任を負いません。また、SonicWallおよび/またはその提携会社がかかる損害の可能性について知らされていた場合でも同様とします。SonicWallおよび/またはその関連会社は、本文書の内容の正確性や完全性に関して、いかなる表明や保証も行わず、また予告なしにいつでも仕様および製品の説明を変更する権利を留保します。SonicWall Inc.および/またはその関連会社は、本文書に記載されている情報の更新について一切責任を負わないものとします。