SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

マルチクラウド環境で企業のリソースにアクセスする際のセキュリティを提供します。いつどこから
アクセスする場合もユーザーやデバイスのアイデンティティ、場所、信頼情報に基づく保護が可能です。

SonicWall SMAは企業活動を支える重要なリソースにいつでも、どこからでも、どのようなデバイスでも、安全にアクセスできるようにする統合型ゲートウェイです。SMAは緻密に調整ができるアクセス制御ポリシーエンジンやコンテキスト判断によるデバイスの許可、アプリケーションレベルでのVPN、シングルサインオンによる高度な認証などの機能を備え、マルチクラウド環境における組織のBYOD体制やモビリティ導入を支援します。

モビリティとBYOD

BYODのような柔軟な業務遂行やサードパーティが提供するアクセスの導入に前向きな組織にとって、SMAはそれらを横断的にカバーし、ポリシーを強制的に適用するための重要なポイントとなります。SMAはクラス最高峰のセキュリティで攻撃面がもたらす脅威を極力減らしつつ、最新の暗号化アルゴリズムと暗号をサポートすることで組織のセキュリティを強固にします。管理者はSonicWallのSMAを利用することでモバイル環境からの安全なアクセスを提供し、アイデンティティに基づく権限を付与できます。そのためエンドユーザーは使用したいビジネスアプリケーションやデータ、リソースに簡単な手続きで素早くアクセスできるようになります。同時に、不正なアクセスやマルウェアから企業ネットワークとデータを守るための、安全性の高いBYODポリシーを策定できます。

クラウドへの移行

SMAは、クラウドへの移行に着手した組織にシングルサインオン（SSO）が可能なインフラストラクチャを提供します。これによりWebポータル1つでハイブリッドなIT環境に置かれたユーザーを認証することが可能です。オンプレミス環境やWeb上、あるいはホストされたクラウド上のいずれに企業リソースが存在している場合でも一貫したシームレスなアクセスが可能であるため、リソースがある場所を意識する必要はありません。また業界を代表する多要素認証技術との統合によって、セキュリティがさらに強化されています。

管理対象サービスプロバイダ

SMAは自社独自のインフラストラクチャをホストする組織にも管理対象サービスプロバイダにも、導入後すぐにお使いいただけるソリューションとして、高度な事業継続性と拡張性を発揮します。アプライアンス1台で最大20,000台の同時接続に対応し、インテリジェンスを備えたクラスタリングによって数十万規模までユーザー数を拡張可能です。SMAをデータセンターでの運用であれば、アクティブ-アクティブクラスタリングと内蔵の動的なロードバランサーの機能により、ユーザーの要望に応じてリアルタイムで最適なデータセンターにグローバルトラフィックを割り当て直すことが可能になり、コスト削減効果を得られます。サービスプロバイダであればダウンタイムを生じることなくサービスを提供できるツールセットを活用することで、極めて高水準のSLAを達成することも可能です。

SMAはユーザーのシナリオに応じて最高のエクスペリエンスと安全性に優れたアクセスを提供できる、IT部門の強力な味方です。堅牢な物理アプライアンスや高性能な仮想アプライアンスとして利用できるSMAは、既存のオンプレミス環境とクラウドインフラストラクチャいずれの用途にも適しています。個人用デバイスを使用するサードパーティや従業員のためにWebベースによる完全クライアントレスのセキュアなアクセスを提供するのも、あるいは管理職向けにあらゆるデバイスタイプで使用できる完全にトンネル化された従来型のクライアントベースのVPNを提供するのも、すべては組織の自由です。SonicWall SMAなら1拠点で5ユーザーが安心してアクセスできるセキュリティを提供したいという要望にも、グローバルな分散ネットワークを利用する数千のユーザーにセキュリティを拡張したいという要望にも応えることができます。

モビリティやBYODの導入に不安を感じることはありません。クラウドへの移行に伴う困難はSonicWall SMAにお任せください。会社を支える人材の力を引き出し、一貫性のあるアクセスエクスペリエンスをお届けします。

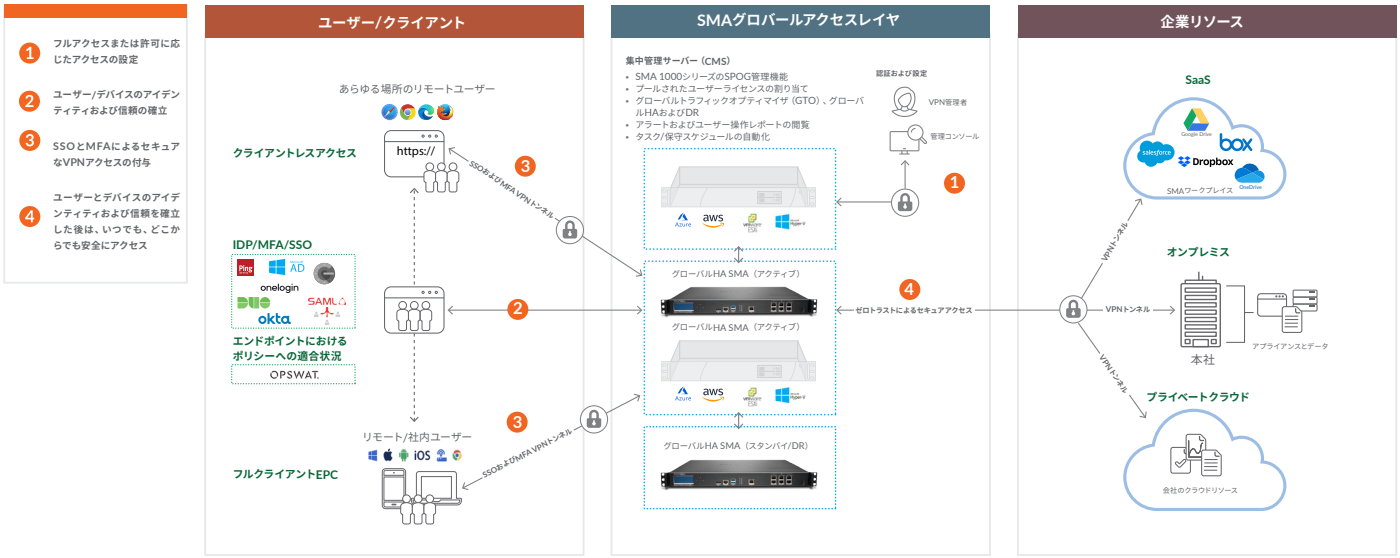
導入効果：

- あらゆるネットワークとクラウドのリソースを「いつでも、どのデバイスからでも、どのアプリケーションからでも」安全に利用できる一元化されたアクセスを実現
- 強力なアクセス制御エンジンできめ細かくポリシーを定義することで、アクセスできるリソースの種類と対象者を制御
- あらゆるSaaSやローカルにホストされているアプリケーションに対して単一のURLでフェデレーションによるシングルサインオンを提供し、生産性を向上
- ハイブリッドIT環境のインフラ要素を統合することでTCOを削減し、アクセス管理に伴う複雑さを低減
- すべての接続デバイスを可視化し、ポリシーおよびエンドポイントの正常性に基づいてアクセスを付与
- Capture ATPサンドボックスの機能でネットワークにアップロードされたファイルを漏れなくスキャンし、マルウェアによる被害を防止
- アドオンのWebアプリケーションファイアウォールの機能でWebベースの攻撃を防御し、PCIへの準拠を実現
- Geo IPの検知やボットネットに対する防御機能を搭載することで、DDoSやゾンビネットワークからの攻撃を阻止
- WebブラウザベースのクライアントレスHTML5によるアクセスを活用することで、エンドポイントデバイスでのエージェントのインストールや管理に付随する負担をかけずに安全なネイティブエージェントの機能を利用。
- リアルタイムの監視と包括的なレポート機能によって的確な意思決定を下すために必要な、実践的な分析情報を獲得
- ESXiやHyper-Vのプライベートクラウド、あるいはAWSやMicrosoft Azureのパブリッククラウド環境に物理アプライアンスや仮想アプライアンスとして展開
- リアルタイムでの需要に応じて動的にアクセスライセンスを発行。エンドポイントには最大限のパフォーマンスと接続遅延の抑制を自動的に指示。
- 内蔵ロードバランサーによりハードウェアやサービスの追加が必要なく、初期費用の削減に貢献。アプライアンスのフェイルオーバー時もユーザー影響なし。
- 事業の停止や特定の時期に固有のアクセスの急増にも、許容量を拡張することで即座に対応。

SMAの展開

いつでも、どこでも、どのデバイスでも安全なアクセスを実現する堅牢なエッジゲートウェイ

SMAはオンプレミス、クラウド、およびハイブリッドデータセンターにおいてホストされる企業リソースへの包括的なエンドツーエンドのセキュアリモートアクセスを提供します。これは、ユーザーとデバイスのアイデンティティと信頼を確立した後に、データ、リソース、アプリケーションへのアクセスを付与するために、アイデンティティベースでのポリシーの強制適用によるアクセス制御、コンテキストを踏まえたデバイス認証、そしてアプリケーションレベルのVPNを適用します。 ESXiやHyper-Vのプライベートクラウド、あるいはAWSやMicrosoft Azureのパブリッククラウド環境において、ハードニングしたLinuxアプライアンスや仮想アプライアンスとして柔軟に展開されます。



SMAクラウド/オンプレミス展開

物理アプライアンスおよび仮想アプライアンスへの柔軟な展開

SonicWall SMAは堅牢かつ高性能なアプライアンスとして展開するだけでなく、共有のコンピューティングリソースを利用する仮想アプライアンスとして展開することで、リソース使用率の最適化や容易なマイグレーション、設備投資の削減などに効果が得られます。マルチコアアーキテクチャを基盤に構築されたハードウェアアプライアンスはSSLアクセラレーションやVPNによるスループット、高機能なプロキシの支援によって高い性能を発揮し、堅牢なセキュアアクセスを実現します。SMAはFIPS 140-2のレベル2認定に対応しているため、規制の厳しい組織や政府機関でもお使いいただけます。SMA仮想アプライアンスもMicrosoft Hyper-V、VMware ESX、AWSなどの主要な仮想プラットフォームやクラウドプラットフォームで、ハードウェアの場合と同等の堅牢なセキュアアクセスを実現します。

複数のアプライアンスで共用できるユーザーライセンス

アプライアンスをグローバルに分散展開している組織では、時差によって生じるユーザーライセンスに対する需要の変化を有効に活用することができます。VPNのフルライセンスを展開している場合でも、あるいはActiveSyncの基本ライセンスを展開している場合でも、同じようにSMAの一元管理によってライセンスの再割り当てが可能です。これにより業務時間外や夜間帯であるという理由でライセンスの使用率が低下した別の地理環境にあるアプライアンスから、ユーザーからの需要がピークに達した管理対象アプライアンスにライセンスを割り当て直すことができます。

コンテキスト認識型のデバイスプロファイリングが可能にするネットワークの可視性

同クラスでは最高レベルのコンテキスト認識を備えた認証機能で、信頼が確立されたデバイスと許可を得たユーザーにのみアクセスを保証します。ノートPCやデスクトップPCに対してはセキュリティソフトウェアやクライアント証明書、デバイスIDの有無も検査されます。モバイルデバイスには脱獄やルート化の状態、デバイスID、証明書のステータス、OSバージョンなどの重要なセキュリティ情報について検査を行ったうえでアクセスが付与されます。ポリシーの要件を満たしていないデバイスはネットワークへのアクセスを拒否され、そのユーザーにはポリシー違反である旨が通知されます。

単一のWebポータルを起点とする一貫性のあるエクスペリエンス

ユーザーはアプリケーションそれぞれのURLを忘れないようにしたり、すべてのブックマークを漏れなく維持管理したりする必要はありません。SMAがユーザーの代わりに集中管理されたアクセスポータルとして、標準的なWebブラウザからミッションクリティカルなアプリケーションにアクセスするためのURLを提供してくれます。ユーザーはブラウザを介してユーザーポータルにログインすることで、お好きなSaaSやローカルアプリケーションにアクセスできます。このポータルはカスタマイズ可能で、単一の画面ですべてを管理できます。ポータルでは特定のエンドポイントデバイスやユーザー、グループに紐づけられたリンクと個人用にカスタマイズされたブックマークのみが表示されます。このポータルはプラットフォームを選ばないという特徴があり、Windows、Mac OS、Linux、iOSおよびAndroidデバイスなどの主要プラットフォームすべてと、それらのデバイス上で動作するさまざまなブラウザに対応しています。

フェデレーションによりSaaSでもローカルアプリケーションでもシングルサインオンが可能

パスワードをいくつも用意する必要がなくなり、パスワードの使いまわしのようなセキュリティ上好ましくない行為を止めることができます。SMAを使用することで、クラウドにホストされているSaaSアプリケーションでも構内や社内にホストされているアプリケーションでもフェデレーション方式のSSOが可能です。SMAによって認証、認可、アカウント管理用の複数のサーバーが統合され、さらに先進の多要素認証技術を利用することでセキュリティを強化しています。セキュアなSSOは、SMAによって正常かつポリシーに適合していることが確認された、認可を受けたエンドポイントデバイスにのみ提供されます。アクセスポリシーエン

ジンの機能によってユーザーには認可されたサーバーだけが見え、正常に認証を通過してはじめてアクセスが付与されるようになります。このソリューションではVPNクライアントを使用する場合でもフェデレーション方式のSSOがサポートされるため、顧客がクライアントベースとクライアントレスどちらのセキュアアクセスを採用しても、シームレスな使用感を提供できます。

セキュリティ侵害と高度な脅威に対する防御手段

SonicWallSMAではアクセスセキュリティの層を厚くすることでセキュリティに対する取組みを改善し、脅威にさらされる攻撃面を小さくします。

- SMAには、管理対象外のエンドポイントを利用するユーザーや企業ネットワーク外のユーザーがアップロードしたファイルをスキャンするSonicWall Capture ATPのクラウドベースによるマルチエンジン式サンドボックスが統合されています。これにより出先にいるユーザーの利用環境をオフィス環境と変わらない水準[1]で、ランサムウェアやゼロデイ攻撃を行うマルウェアなどの高度な脅威から守ることができます。
- SonicWall Webアプリケーションファイアウォールサービスは企業に手頃な料金で統合度の高いソリューションを提供し、社内で利用しているWebベースのアプリケーションを安全に保ちます。これにより顧客が抱えるデータの機密性を保証し、万一社内のWebサービスが不正入手した情報によるユーザーや悪意のあるユーザーからのアクセスを受けた場合でも、サービスの悪用を防ぐことができます。
- さらにGeo-IPやボットネットの検知機能で、DDoS攻撃やゾンビネットワークによる攻撃、感染被害を受けてボットネットとして動作するエンドポイントなどから組織を保護します。

安全性とシームレスを両立するブラウザベースのクライアントレスアクセス

SonicWall SMAの「クライアントレス」という特徴は、リモートアクセス用のファットクライアントのコンポーネントを管理者の手でコンピュータにインストールする必要がないということを意味します。これによりJavaなどに依存することが一切なくなり、ITにとって負荷となる要素がなくなります。つまり事前にインストールしたり設定したりといった作業が不要になり、許可されたユーザーであれば好きなコンピュータを使用して、世界中どこからでも安全に企業リソースへのリモートアクセスができることになります。セキュアアクセスのもっとも純粋な形態はHTML5を使用したブラウザベースに限定するもので、シームレスで一体的な使用感をユーザーに提供します。

「Always On」の実現

SMAのAlways On VPN（常時接続VPN）機能は管理下に置かれたWindowsデバイスにシームレスなユーザーエクスペリエンスを提供します。管理者は認可されたエンドポイントクライアントがパブリックネットワークや信頼されていないネットワークを検知すると、自動でVPN接続が確立されるように設定できます。Windowsデバイスへのシングルログインイベントによって、ユーザーには企業リソースへの安全な接続が提供されます。ユーザーが各自のVPNクライアントにログインしたり、他にもパスワードを管理したりする必要はありません。この機能があれば、モバイルユーザーはオフィスにいるかのような感覚でミッションクリティカルなリソースにシームレスにアクセスできます。IT管理者にとっては管理対象デバイスの管理が容易になり、組織のセキュリティ対策の強化につながります。

直感的な管理機能と包括的なレポート機能

SonicWallでは直感的に操作可能なWebベースの管理プラットフォームである集中管理サーバー（CMS）をご用意しています。アプライアンスの効率的な管理に役立つだけでなく、豊富なレポート機能もお使いいただけます。GUIも扱いやすく、アプライアンスやポリシーを個別に管理する場合も複数を対象に管理する場合も明快な使用感が得られます。各ページには管理下にある全マシンの設定状況が表示されます。アクセスポリシーや設定の作成および監視には、統合されたポリシー管理機能を活用していただけます。ユーザーからデバイス、アプリケーション、データ、サーバーやネットワークに至るまで、たった1つのポリシーでアクセスを制御可能です。ITは日常的な所定のタスクやスケジュールに沿った作業を自動化することでセキュリティチームは反復的なタスクから解放され、インシデント対応のような戦略的なセキュリティ業務に集中できるようになります。また扱いやすいレポート機能やログの集中管理機能も備えているため、ユーザーのアクセス傾向やシステム全体の正常性について確かな理解を得ることができます。

サービスに24時間365日の可用性

組織には自社が提供するサービスの信頼性を高水準に保ったまま運用し、ミッションクリティカルなアプリケーションにいつでも安全にアクセスできるよう維持することが求められます。SMAアプライアンスは単独のデータセンターで従来のアクティブ-パッシブな高可用性（HA）を確保する用途にも、ローカルにあるデータセンターや分散配置されているデータセンターでアクティブ-アクティブまたはアクティブ-スタンバイのクラスタリングによってグローバルな規模でHAを確保する用途にも対応できます。どちらのHAモデルも、サービスに影響を及ぼさないフェイルオーバーのしくみやセッションの継続性を備えており、ユーザーに負担を感じさせずにサービスを提供できます。

需要に合ったVPNクライアントの展開

さまざまなVPNクライアントの中からポリシーを適用したセキュアなリモートアクセスを、ノートPC、スマートフォン、タブレットなどのさまざまなエンドポイントに提供します。

VPNクライアント	サポート対象のOS	サポート対象のSMAモデル	主要な機能
Mobile Connect	iOS、OS X、Android、Chrome OS、Windows 10	すべてのモデル	アプリのVPN単位での生体認証やエンドポイント制御の強制
Connect Tunnel（シンクライアント）	Windows、Mac OS、Linux	6200、6210、7200、7210、8200v、9000	強力なエンドポイント制御による完全な「インオフィスエクスペリエンス」
NetExtender（シンクライアント）	WindowsおよびLinux	210、410、500v	きめ細かいアクセスポリシーの強制適用やネイティブクライアントを介したネットワークアクセスの拡張

ロードバランサー内蔵で初期費用を削減

SMAアプライアンスには負荷分散機能が搭載されているため、中規模の事業者や大企業での導入にも応えられる拡張性を有しています。厳選されたSMAアプライアンスのモデルは動的な負荷分散機能で的確にセッションの負荷を配分し、要求に即してリアルタイムにユーザーライセンスを割り当てることが可能です。別途ロードバランサーに投資する必要がないため、初期投資の抑制につながります。

未曾有の事象に備える

アクセストラフィックの急増に対処しつつ、セキュリティを損なわずコスト管理も維持できてこそ完璧な事業継続ソリューションであり、完璧なDRソリューションです。SonicWall SMA用のスパイクライセンスパックはアドオン型のライセンスで、ユーザー数を最大値まで即座に拡張でき、シームレスな事業継続体制を実現できます。スパイクライセンスは保険契約のような使い方ができ、先々の計画的または計画外の急増に対しユーザー数の追加に対応します。数十単位のユーザーはもちろん数百という単位での追加も可能です。

機能

高度な認証

フェデレーションにによるサインオン[2]	SMAはSAML 2.0認証を使用して単一ポータル経由でのフェデレーション方式のSSOをオンプレミスとクラウド両方のリソースに対して実現します。同時に、複数のサービスを利用する多要素認証を強制することでセキュリティを強化します。
多要素認証	X.509デジタル証明書 サーバー側とクライアント側のデジタル証明書 RSA SecurID、Dell Defender、Google Authenticator、Duo Security、その他のワンタイムパスワード/2要素認証トークン 共通アクセスカード（CAC） 2つまたは複数のサービスによる認証 Captchaサポート、ユーザー名/パスワード
SAML認証	SMAをSAMLアイデンティティプロバイダ（IdP）やSAMLサービスプロバイダ（SP）、プロキシとして既存のオンプレミスIdPに設定し、SAML 2.0認証を使用したフェデレーション方式のシングルサインオン（SSO）が可能です。
認証リポジトリ	SMAは業界標準のリポジトリとのシンプルな統合を提供し、ユーザーアカウントとパスワードを簡単に管理できるようにします。 RADIUS、LDAP、またはActive Directoryの認証リポジトリに基づいて、ネストされたグループも含むユーザーグループに動的にメンバーを追加できます。 特定の認可やデバイスの登録状況確認において共通またはカスタムのLDAP属性を確認させることができます。
レイヤ3~7を対象とするアプリケーションプロキシ	SMAでは柔軟なプロキシオプションを用意しています。たとえばExchangeにアクセスするにあたってベンダーには直接プロキシを、請負業者にはリバースプロキシをそれぞれ経由してもらい、従業員にはActiveSyncを利用してもらうことが可能です。
リバースプロキシ	管理者は認証付きの強力なリバースプロキシサービスを利用することでアプリケーションの処理をオフロードするポータルやブックマークを設定し、ユーザーにRDPやHTTPを含むリモートのアプリケーションおよびリソースへのシームレスな接続を提供します。この機能はIE、Chrome、Firefoxを始めとするすべてのブラウザをサポートします。
Kerberosによる強制的な権限代行	SMAは既存のKerberosインフラストラクチャを活用して認証サポートを提供します。これによりサービスを代行させるためにフロントエンドサービスを信頼する必要はありません。

アクセス管理

アクセス制御エンジン（ACE）	管理者は組織のポリシーに基づいてアクセスの許可または拒否を決定でき、検疫を行うセッションでは修復アクションを設定できます。ACEのオブジェクトベースのポリシーでは、ネットワーク、リソース、アイデンティティ、デバイス、アプリケーション、データ、時間といった要素を活用できます。
エンドポイント制御（EPC）	EPCを利用することで管理者は接続を試みる側のデバイスの正常性に基づいてアクセス制御のルールを適用することができます。OSと深いレベルで統合することで、多くの要素を結合し、タイプ分類とリスク要因評価を実現しています。EPCによる調査は、事前に定義しておいたアンチウィルス、パーソナルファイアウォール、アンチスパイウェアソリューションの包括的なリストを使用することでWindows、Mac、Linuxプラットフォームのデバイスプロフィール設定を簡略化します。
アプリケーションアクセス制御（AAC）	各アプリのトンネルを介してどのモバイルアプリケーションからネットワーク上のどのリソースにアクセスできるかを、管理者が定義できます。AACポリシーはクライアントとサーバーの両方に適用できるため、境界における防御を強固にすることが可能です。

優れたセキュリティ

レイヤ3 SSL VPN	SMAシリーズはいかなる環境で動作するさまざまな種類のクライアントデバイスにも、高性能のレイヤ3トンネル機能を提供します。
暗号機能のサポート	セッション持続時間を調整可能 暗号アルゴリズム：AES 128 + 256 ビット、Triple DES、RC4 128ビット ハッシュ方式：SHA-256 楕円曲線DSA（ECDSA）
高度暗号化のサポート	SMAアプライアンスは初期設定の暗号そのままの状態でも強固なセキュリティを誇り、コンプライアンス対策に有効ですが、パフォーマンスやセキュリティ強度、互換性の追求など、目的に合わせた調整を管理者が行えます。
セキュリティに関する認定	FIPS 140-2レベル2、ICSA SSL-TLS認定取得済み。Common Criteria、UC-APL認定審査中
セキュアなファイル共有	ランサムウェアのような未知の攻撃やゼロデイ攻撃をゲートウェイで阻止し、自動的に修復も行います。管理対象外のエンドポイントから企業ネットワークに対してセキュアアクセスでアップロードされたファイルは、クラウドベースのマルチエンジン式Capture ATPの検査対象となります。
Webアプリケーションファイアウォール（WAF）	プロトコルに対する攻撃やWebベースの攻撃を防ぎ、金融や医療、Eコマースなどの業務を扱う事業者がOWASPが挙げる上位10件のリスクへの対処やPCIへの準拠を達成するのに効果を発揮します。
Geo IPの検知とボットネットの防御	Geo IPの検知とボットネットの防御機能によって、さまざまな地理的位置からのユーザーアクセスを顧客の手で許可したり、あるいは制限したりするしくみが実現します。
TLS 1.3のサポート	従前の暗号化プロトコルにまつわる複雑さを解消しつつ、セキュリティと性能の両面を向上させます。

直感的なユーザーエクスペリエンス

Always On VPN	会社支給のWindowsデバイスから企業ネットワークに対して自動的にセキュアな接続を確立することで、セキュリティの向上とトラフィックの可視化、コンプライアンスの維持を実現します。
セキュアネットワーク検知（SND）	ネットワーク把握機能を有するSMAのVPNクライアントは、構内や社内のネットワーク外にいる状態を検知して自動的にVPNに再接続します。デバイスが信頼しているネットワーク上にくると、再び元の状態に戻ります。
リソースへのクライアントレスアクセス	SMAはRDP、ICA、VNC、SSH、Telnetプロトコルを提供するHTML5ブラウザエージェントを利用することで、リソースに対してクライアントレスでのセキュアなアクセスを実現します。
シングルサインオンポータル	WorkPlaceポータルは扱いやすくカスタマイズ可能な、シングルペインによる表示を特徴とします。ハイブリッドなIT環境におけるあらゆるリソースに、シングルサインオン（SSO）で安全にアクセス可能です。何度もログインしたり、VPNを増やす必要はありません。
レイヤ3トンネリング	SSL/TLSトンネリングでスプリットトンネルモードにするか、すべてリダイレクトモードにするかを選択できるほか、オプションのESPフォールバックでパフォーマンスを最大化するかを管理者が選べます。
HTML5ファイルエクスプローラー[1]	モダンなファイルブラウザを利用して任意のWebブラウザから簡単にファイル共有ができます。
モバイルOS統合	Mobile ConnectはすべてのOSプラットフォームでサポートされるため、モバイルデバイスの選択肢が広がります。

耐障害性

グローバルトラフィックオプティマイザ（GTO）	SMAはユーザーに影響を及ぼすことなくグローバル規模でトラフィックの負荷分散が可能です。トラフィックは最適かつパフォーマンスが優れているデータセンターにルーティングされます。
動的な高可用性[2]	SMAはアクティブ/パッシブの構成だけでなく、高可用性に優れたアクティブ/アクティブの構成もサポートし、単独のデータセンターへの配置にも、地理的に離れた複数のデータセンターへの配置にも対応します。
ユニバーサルセッション持続機能[1]	ユーザーにフェイルオーバーによる影響を及ぼすことなくサービスを維持できます。SMAアプライアンスがオフラインの状態になると、インテリジェンスを備えたクラスタリングによってユーザー各自のセッションデータが割り当てしなおされます。その際の再認証の手続きは不要です。
拡張可能なパフォーマンス	SMAアプライアンスは同機を複数展開することでパフォーマンスを飛躍的に拡張し、単一障害点をなくすことができます。水平クラスタリングはSMAアプライアンスの物理展開と仮想展開の混在構成を全面的にサポートしています。
動的なライセンス付与	ユーザーライセンスを個々のSMAアプライアンスに適用する必要はありません。ユーザーには需要に応じて管理対象デバイスの割り当てと調整が動的に行われます。

集中管理と監視

集中管理システム (CMS)	CMSはSMAの全機能に対してWebベースの集中管理を提供します。
カスタムアラート	SNMPトラップが生成されるようにアラートを設定し、お好きなITインフラネットワーク管理システム (NMS) で監視できます。管理者はCapture　ATPのファイルスキャンとディスク使用量に関するアラートを設定し、迅速な対応が取れるように備えることもできます。
リアルタイムダッシュボード	カスタマイズできるリアルタイムのダッシュボードを活用すれば、IT管理者がアクセスの問題を速やかに診断してトラブルシューティングに役立てられる貴重な分析情報を得られます。
SIEM統合	中心的な役割のSIEMデータコレクターにリアルタイムで出力されるデータは、セキュリティチームがイベント駆動型の事象を関連付け、特定ユーザーまたは特定アプリケーションのエンドツーエンドのワークフローを把握するのに役立ちます。セキュリティインシデントの管理とフォレンジック分析の際には、この機能が非常に効果的です。
スケジューラ	スケジューラを活用するとポリシーの配布や構成情報の複製、サービス再起動のような保守タスクに一切介入することなく計画的に実行することができます。

拡張性

管理API	管理APIを利用することで、単一のSMA環境やグローバルなCMS環境にあるすべてのオブジェクトに対して、完全にプログラムによる管理が可能になります。
エンドユーザーAPI	エンドユーザーAPIを利用することで、あらゆるログオンや認証、エンドポイントのワークフローを完全に制御できるようになります。
2要素認証 (2FA)	Google Authenticator、Microsoft Authenticator、Duoセキュリティなどの業界を代表する時間ベースのワンタイムパスワード (TOTP) ソリューションと統合することで2FAを利用できます。
MDM統合	AirwatchやMobile Ironなどの先進的なエンタープライズモバイル管理 (EMM) 製品と統合できます。
その他のサードパーティ系統合	OPSWATなどの業界を代表するベンダーとの統合によって高度な脅威防御を実現できます。

[1] SMA OS 12.1以降で利用可

[2] SMA 12.1で機能を強化

機能概要（モデル別の比較）

分類	機能	210	410	500v	6210	7210	8200v
展開	オペレーティングシステム	SMA 10.2	SMA 10.2	SMA 10.2	SMA 12.4	SMA 12.4	SMA 12.4
	サポート対象のハイパーバイザ	–	–	VMware ESXi/ Microsoft Hyper-V	–	–	VMware ESXi/ Microsoft Hyper-V
	サポート対象のパブリッククラウドプラットフォーム	–	–	AWS/Azure	–	–	AWS/Azure
スループット	複数同時ユーザーセッションの最大数	50	250	250	2,000	10,000	5,000
	SSL/TLSの最大スループット	560 Mbps	844 Mbps	186 Mbps	800 Mbps	5.0 Gbps	1.58 Gbps
クライアントアクセス	レイヤ3トンネル	•	•	•	•	•	•
	スプリットトンネルとすべてリダイレクト	•	•	•	•	•	•
	Always On VPN	•	•	•	•	•	•
	自動ESPカプセル化	–	–	–	•	•	•
	HTML5（RDP、VNC、ICA、SSH、Telnet、Network Explorer）	•	•	•	•	•	•
	セキュアネットワーク検知	–	–	–	•	•	•
	ファイルブラウザ（CIFS/NFS）	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	オンデマンド方式のトンネル	–	–	–	•	•	•
	Chrome/Firefox拡張機能	–	–	–	•	•	•
	CLIトンネルのサポート	–	–	–	•	•	•
	Mobile Connect（iOS、Android、Chrome、Win 10、Mac OSX）	•	•	•	•	•	•
	Net Extender（Windows、Linux）	•	•	•	–	–	–
	Connect Tunnel（Windows、Mac OSX、Linux）	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
モバイルアクセス	アプリ毎のVPN	–	–	–	•	•	•
	アプリ制御の強制適用	–	–	–	•	•	•
	アプリIDの検証	–	–	–	•	•	•
ユーザーポータル	ブランディング	•	•	•	•	•	•
	カスタマイズ	–	–	–	•	•	•
	ローカリゼーション	•	•	•	•	•	•
	ユーザー定義のブックマーク	•	•	•	•	•	•
	カスタムURLのサポート	•	•	•	•	•	•
	SaaSアプリケーションのサポート	–	–	–	•	•	•
セキュリティ	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B暗号	–	–	–	•	•	•
	動的EPC検査	•	•	•	•	•	•
	ロールベースのアクセス制御（RBAC）	–	–	–	•	•	•
	エンドポイントへの登録	•	•	•	•	•	•
	安全なファイル共有（Capture ATP）	•	•	•	•	•	•
	エンドポイントでの検疫	•	•	•	•	•	•
	OSCP CRL検証	–	–	–	•	•	•
	暗号の選択	–	–	–	•	•	•
	PKI証明書とクライアント証明書	•	•	•	•	•	•
	Geo IPフィルタ	•	•	•	–	–	–
	ボットネットフィルタ	•	•	•	–	–	–
	フォワードプロキシ	•	•	•	•	•	•
	リバースプロキシ	•	•	•	•	•	•
認証サービスとアイデンティティサービス	SAML 2.0	–	–	–	•	•	•
	LDAP、RADIUS	•	•	•	•	•	•
	Kerberos（KDC）	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML アイデンティティプロバイダ（IdP）	•	•	•	•	•	•
	生体認証デバイスのサポート	•	•	•	•	•	•
	iOSのFace IDのサポート	•	•	•	•	•	•
	2要素認証（2FA）	•	•	•	•	•	•
	多要素認証（MFA）	–	–	–	•	•	•

機能概要（モデル別比較（続き））

分類	機能	210	410	500v	6210	7210	8200v
認証サービスとアイデンティティサービス（続き）	チェーン認証	–	–	–	•	•	•
	メールまたはSMSを介したワンタイムパスワード（OTP）	•	•	•	•	•	•
	共通アクセスカード（CAC）のサポート	–	–	–	•	•	•
	X.509証明書のサポート	•	•	•	•	•	•
	Captcha統合	–	–	–	•	•	•
	リモートからのパスワード変更	•	•	•	•	•	•
	フォームベースSSO	•	•	•	•	•	•
	フェデレーションSSO	–	–	–	•	•	•
	セッション持続機能	–	–	–	•	•	•
	自動ログオン	•	•	•	•	•	•
アクセス制御	グループAD	•	•	•	•	•	•
	LDAP属性	•	•	•	•	•	•
	ジオロケーションポリシー	•	•	•	–	–	–
	継続的なエンドポイント監視	•	•	•	•	•	•
管理	管理インターフェイス（ethernet）	–	–	–	•	•	•
	管理インターフェイス（コンソール）	–	–	–	•	•	•
	HTTPS経由の管理	•	•	•	•	•	•
	SSH経由の管理	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	SyslogとNTP	•	•	•	•	•	•
	使用状況の監視	•	•	•	•	•	•
	構成のロールバック	•	•	•	•	•	•
	集中管理	–	–	–	•	•	•
	集中管理によるレポート機能	–	–	–	•	•	•
	管理用REST API	–	–	–	•	•	•
	認証用REST API	–	–	–	•	•	•
	RADIUSアカウント管理	–	–	–	•	•	•
	タスクの計画実行	–	–	–	•	•	•
	集中管理によるセッションライセンスの付与	–	–	–	•	•	•
	イベント駆動型の監査機能	–	–	–	•	•	•
ネットワーク機能	IPv6	•	•	•	•	•	•
	グローバルロードバランサー	–	–	–	•	•	•
	サーバーロードバランサー	•	•	•	–	–	–
	TCPの状態の複製	•	•	•	•	•	•
	クラスターの状態のフェイルオーバー	–	–	–	•	•	•
	アクティブ/パッシブ方式による高可用性	–	•	•	•	•	•
	アクティブ/アクティブ方式による高可用性	–	–	–	•	•	•
	水平方向の拡張性	–	–	–	•	•	•
	単一または複数のFQDN	–	–	–	•	•	•
	レイヤ3～7対応のスマートトンネルプロキシ	•	•	•	•	•	•
	レイヤ7のアプリケーションプロキシ	•	•	•	•	•	•
統合機能	2FA TOTPのサポート	•	•	•	•	•	•
	EMMおよびMDM製品のサポート	–	–	–	•	•	•
	SIEM製品のサポート	–	–	–	•	•	•
	TPAMパスワードヴォールト	–	–	–	•	•	•
	ESXハイパーバイザのサポート	–	–	•	–	–	•
	Hyper-Vハイパーバイザのサポート	–	–	•	–	–	•
ライセンスオプション	サブスクリプションベースのライセンス	–	–	–	•	•	•
	サポート付き永久ライセンス	•	•	•	•	•	•
	Webアプリケーションファイアウォール（WAF）	•	•	•	–	–	–
	スパイクライセンス	•	•	•	•	•	•
	階層ライセンス	–	–	–	•	•	•
	バーチャルアシスト	•	•	•	–	–	–

* VPNクライアントについて詳しくは、https://www.sonicwall.com/en-us/products/remote-access/vpn-clientをご覧ください。

ハイエンドアプライアンスへのアップグレードによる利点

パフォーマンスの強化 | スループットの向上 | 高度な機能 | より高い拡張性

アプライアンスの仕様

Secure Mobile Access（SMA）専用の豊富なアプライアンスをご用意しています。仮想および物理アプライアンスの柔軟な展開オプションからお選びください。

物理アプライアンスの仕様

パフォーマンス	SMA 210	SMA 410	SMA 6210	SMA 7210
同時セッション/ユーザー数	最大50	最大250	最大2,000	最大10,000
SSL VPNのスループット*（最大CCU）	560 Mbps	844 Mbps	最大800 Mbps	最大5.0 Gbps
フォームファクタ	1U	1U	1U	1U
寸法	16.92 x 10.23 x 1.75インチ (43 x 26 x 4.5 cm)	16.92 x 10.23 x 1.75インチ (43 x 26 x 4.5 cm)	17.0 x 16.5 x 1.75インチ (43 x 41.5 x 4.5 cm)	17.0 x 16.5 x 1.75インチ (43 x 41.5 x 4.5 cm)
アプライアンスの重量	11ポンド (5 kg)	11ポンド (5 kg)	17.7ポンド (8 kg)	18.3ポンド (8.3 kg)
暗号化データのアクセラレーション (AES-NI)	NO	NO	YES	YES
管理専用ポート	NO	NO	YES	YES
SSLアクセラレーション	NO	NO	YES	YES
ストレージ	4 GB（フラッシュメモリ）	4 GB（フラッシュメモリ）	2 x 1TB SATA：RAID 1	2 x 1TB SATA：RAID 1
インターフェイス	(2) GB Ethernet、(2) USB、(1) コンソール	(4) GB Ethernet、(2) USB、(1) コンソール	(6) ポート 1 GE、(2) USB、(1) コンソール	(6) ポート 1 GE (2) ポート 10 Gb、SFP+、(2) USB、(1) コンソール
メモリ	4 GB	8GB	8 GB DDR4	16GB DDR4
TPMチップ	NO	NO	YES	YES
プロセッサ	4コア	8コア	4コア	4コア
MTBF（@ 25°Cまたは77°F）（単位は時間）	61,815	60,151	70,127	129,601
動作条件および認証への準拠	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
電源	固定電源	固定電源	固定電源	冗長電源、ホットスワップ対応
定格入力	100～240VAC 50～60MHz	100～240VAC 50～60MHz	100～240VAC、1.1 A	100～240VAC、1.79 A
消費電力	26.9 W	31.9 W	77 W	114 W
総発熱量	92 BTU	109 BTU	264 BTU	389 BTU
環境規格	WEEE、EU RoHS、China RoHS			
非動作時耐衝撃	110 g、2 ミリ秒			
エミッション規格	FCC、ICES、CE、C-Tick、VCCI；MIC			
安全規格	TUV/GS、UL、CE PSB、CCC、BSMI、CB scheme			
動作温度	0°C～40°C（32°F～104° F）			
FIPS認定	NO	NO	FIPS 140-2 レベル 2、改ざん防止保護機能を含む	

** スループットのパフォーマンスは展開条件および接続環境によって異なる場合があります。公表値は社内ラボの条件によります*

仮想アプライアンスの仕様

仕様	SMA 500v（ESX/ESXi/Hyper-V）	SMA 8200v（ESX/ESXi/Hyper-V）
同時セッション	最大250ユーザー	最大5000
SSL-VPN スループット*（最大CCU）	最大186 Mbps	最大1.58 Gbps
割り当てメモリ	2 GB	8 GB
プロセッサ	1コア	4コア
SSLアクセラレーション	NO	YES
適用ディスクサイズ	2 GB	64 GB（デフォルト）
インストール済みオペレーティングシステム	Linux	ハードニング済みLinux
管理専用ポート	NO	YES

** スループットのパフォーマンスは展開条件および接続環境によって異なる場合があります。公表値は社内ラボの条件によります。Hyper-V上のSMA 8200vは最大5000件まで複数同時セッション数を拡張可能。Windows Server 2016でのSMA OS 12.1動作時のSSL-VPNスループットは最大1.58 Gbps*

パートナーイネーブルサービス

SonicWallソリューションの計画、展開、最適化についてお困りですか。SonicWallアドバンスドサービスパートナーは世界レベルの高度なサービスを提供するためのトレーニングを受けています。詳しくはwww.sonicwall.com/PESをご覧ください。

SonicWallについて

SonicWallは27年以上にわたってサイバー犯罪と戦い、世界中の中小企業や各種事業組織、政府機関を守り続けています。受賞歴のある当社のリアルタイム侵害検出・防止ソリューションは、SonicWall Capture Labsの研究によってその効果が裏付けられています。このソリューション群は、実に215以上の国と地域で、100万以上のネットワークとその中の電子メールやアプリケーション、データを保護しています。これによって多くの組織がより効果的に稼働し、セキュリティ上の懸念を軽減しています。詳しくは、www.sonicwall.comをご覧いただくか、Twitter、LinkedIn、Facebook、Instagramで当社をフォローしてください

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
その他の情報については、当社のウェブサイトをご覧ください。
www.sonicwall.com

© 2020 SonicWall Inc. ALL RIGHTS RESERVED.SonicWallは、SonicWall Inc.および／またはその関連会社の米国および／またはその他の国における登録商標です。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。
Datasheet-SecureMobileAccess-US-VG-1834