SONICWALL

SonicWall Secure Mobile Access (SMA)

モビリティ、BYOD、クラウド移行の課題に直面している組織に向けた
統合セキュアアクセスゲートウェイ

SonicWall SMA は、時間や場所、デバイスを問わずにミッションクリティカルな企業リソースにアクセスを可能にする、統合セキュアアクセスゲートウェイです。SMA のきめ細かなアクセス制御ポリシーエンジン、コンテキスト対応デバイス認証、アプリケーションレベル VPN、およびシングルサインオンによる高度な認証により、組織は、ハイブリッドな IT 環境における BYOD（私物端末の業務利用）とモビリティに対応することができます。

モビリティと BYOD

BYOD、柔軟な勤務形態、サードパーティによるアクセスへの対応を図る組織にとって、SMA はそのすべてにおける重要な実施ポイントとなります。SMA はクラス最高のセキュリティを実現して既知の脅威を最小化し、最新の暗号と暗号化アルゴリズムをサポートすることで組織のセキュリティを強化します。SonicWall SMA により、管理者はセキュアなモバイルアクセスと役割ベースの権限をプロビジョニングすることができます。そのため、エンドユーザーは必要とする業務のアプリケーション、データ、リソースに容易かつ迅速にアクセスできるようになります。それと同時に、組織はセキュアな BYOD ポリシーを導入し、不正アクセスやマルウェアから企業ネットワークと企業データを保護することができます。

クラウドへの移行

クラウドへの移行に取り組んでいる組織は、単一の Web ポータルを使用してハイブリッドな IT 環境のユーザーを認証する、SMA のシングルサインオン (SSO) インフラストラクチャを活用できます。オンプレミス、Web ベース、ホスト型クラウドのすべてにわたって、企業リソースへのシームレスで一貫性のあるアクセスが実現します。さらに、業界をリードする多要素認証テクノロジーと SMA が統合することでセキュリティが強化されています。

マネージドサービスプロバイダ

独自のインフラをホストしている組織とマネージドサービスプロバイダのどちらに対しても、SMA は、ビジネスの高度な継続性と拡張性を実現する、すぐに使用可能なソリューションを提供します。SMA は、単一アプライアンスで最大 2 万の同時接続をサポートし、インテリジェントクラスタリングによってユーザー数を数十万規模で拡張できます。データセンターは、アクティブ / アクティブクラスタリングと標準装備の動的なロードバランサーでコストを削減できます。このロードバランサーは、ユーザーの需要に基づいて最適なデータセンターにグローバルトラフィックをリアルタイムで再配分します。サービスプロバイダは SMA ツールセットによりダウンタイムのないサービスを提供し、非常に積極的な SLA を履行できます。

SMA により、IT 部門はユーザーシナリオに応じた最良のエクスペリエンスと最もセキュアなアクセスを提供することができます。堅牢な物理アプライアンスまたは強力な仮想アプライアンスとして、SMA は既存の IT インフラストラクチャにシームレスに適合します。組織は、サードパーティや個人所有デバイスを使用する従業員向けに、クライアントをまったく必要としない、Web ベースのさまざまなセキュアアクセス方法を選択できます。企業幹部向けには、すべてのデバイスタイプにわたる、従来型のクライアントベースのフルトンネル VPN アクセスを選ぶこともできます。1 つの場所から 5 ユーザーに信頼できるセキュアなアクセスを提供する場合でも、世界各地に分散しているデータセンターでユーザーを数千まで増やす場合でも、SonicWall SMA はソリューションを提供できます。

SonicWall SMA により、組織はモビリティと BYOD を恐れることなく受け入れて、クラウドへ容易に移行することができます。SMA は、従業員の処理能力を高めて一貫性のあるアクセスを実現します。

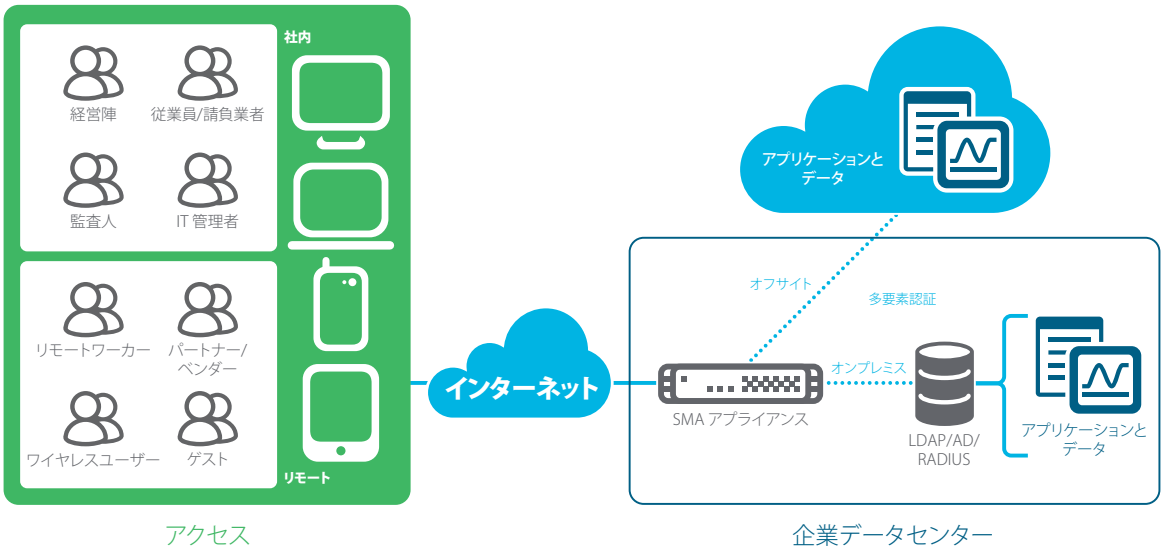
導入効果：

- 「時間、デバイス、アプリケーションを問わない」安全なアクセスを実現する、すべてのネットワークリソースとクラウドリソースへの統合アクセス
- 堅牢なアクセス制御エンジンでポリシーをきめ細かく定義し、誰にどのリソースへのアクセス権を与えるかを制御
- SaaS アプリケーションやローカルにホストされるアプリケーションで単一 URL によるフェデレーテッドシングルサインオンを実現し、生産性を向上
- ハイブリッドな IT 環境のインフラストラクチャコンポーネントを統合することで、TCO を削減してアクセス管理の複雑さを軽減
- すべての接続デバイスを可視化し、エンドポイントの正常性とポリシーに基づいてアクセスを許可
- ネットワークにアップロードされたファイルを Capture ATP サンドボックスですべてスキャンすることでマルウェアの侵入を阻止
- Web アプリケーションファイアウォールのアドオンにより、Web ベースの攻撃の防御、PCI 準拠を実現
- Geo IP 検出とボットネット対策で DDoS 攻撃やゾンビ攻撃を阻止
- Web ブラウザベースのクライアントレス HTML5 アクセスを使用して、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とメンテナンスに伴うオーバーヘッドなしにセキュアなネイティブエージェント機能を実現
- リアルタイム監視と包括的なレポート機能により、適切な意思決定に必要な実行可能な洞察を獲得
- 業務に応じた柔軟な仮想 / 物理アプライアンスオプションによる容易な導入
- リアルタイムの需要に基づくアクセスライセンスの動的な発行を可能にし、パフォーマンスが最も高く、レイテンシが最も低い接続へのエンドポイントの方向付けを自動化
- ユーザーに影響を与えないアプライアンスのフェイルオーバを実現しつつ、ハードウェアやサービスの追加が不要な標準装備の負荷分散機能で先行投資コストを削減
- キャパシティを即座に調整することで業務の中断や季節的な需要の急増に対処

SMA アプライアンスとその導入

時間や場所、デバイスを問わずにセキュアなアクセスを実現する堅牢なエッジゲートウェイ

SMA は、デバイスを問わずにネットワークリソースとクラウドリソースへの安全なアクセスを実現する、高度なアクセスセキュリティゲートウェイです。SMA では、堅牢な Linux ベースのアプライアンスにより、企業リソースへのリモート / モバイルアクセスに、一元化されたきめ細かいポリシーベースの管理が適用されます。堅牢な物理アプライアンスまたは強力な仮想アプライアンスとして、SMA は既存の IT インフラストラクチャにシームレスに適合します。



SMA ソリューションは、すべてのユーザー、デバイス、アプリケーションに安全なアクセスを提供します。

物理 / 仮想アプライアンスによる柔軟な導入

SonicWall SMA は、堅牢で高性能なアプライアンスとして、または共用コンピューティングリソースを活用する仮想アプライアンスとして導入し、使用効率の最適化、容易な移行、資本コストの削減を図ることができます。ハードウェアアプライアンスは、SSL アクセラレーション、VPN スループット、強力なプロキシでハイパフォーマンスを実現するマルチコアアーキテクチャで構築されており、堅牢でセキュアなアクセスを提供します。規制下にある組織や連邦組織に対応するために、SMA は FIPS 140-2 レベル 2 認定も満たしています。SMA 仮想アプライアンスも同様に、Microsoft Hyper-V、VMware ESX などの主要な仮想プラットフォームで堅牢なセキュアアクセス機能を提供します。

アプライアンス間で共有されるユーザーライセンス

アプライアンスが世界各地に分散している組織は、時差によってユーザーライセンスの需要が流動的になることで恩恵を受けます。組織が VPN の完全ライセンスまたは ActiveSync の基本ライセンスのいずれのライセンスを導入している場合でも、SMA の中央管理により、勤務時間外または夜間のために使用率が低下している他地域のアプライアンスから、ユーザーの需要がピークに達している管理対象のアプライアンスにライセンスが再配分されます。

コンテキスト対応デバイスプロファイルによるネットワークの可視化

クラス最高のコンテキスト対応認証により、信頼できるデバイスと許可されたユーザーへのアクセスのみが許可されます。ノートパソコンと PC でも、セキュリティソフトウェア、クライアント証明書、デバイス ID の有無が照会されます。モバイルデバイスでは、ジェイルブレイクやルートステータス、デバイス ID、証明書ステータス、OS バージョンなどの必須セキュリティ情報を照会してからアクセスが許可されます。ポリシー要件を満たしていないデバイスはネットワークアクセスが許可されず、ユーザーには不遵守が通知されます。

単一の Web ポータルによる一貫したエクスペリエンス

ユーザーは、個々のアプリケーションの URL をすべて記憶して包括的なブックマークを維持する必要がなくなります。SMA が提供する一元化されたアクセスポータルにより、ユーザーは標準の Web ブラウザを使用して、ミッションクリティカルなすべてのアプリケーションに 1 つの URL を介してアクセスできます。ユーザーがブラウザを使用してログオンすると、カスタマイズ可能な Web ユーザーポータルがブラウザウィンドウに表示され、SaaS アプリケーションやローカルアプリケーションへのアクセスが一元的に可視化されます。このポータルには、特定のエンドポイントのデバイス、ユーザーまたはグループに関連するリンクやパーソナライズされたブックマークだけが表示されます。このポータルはプラットフォーム非依存であり、Windows、Mac OS、Linux、iOS、Android などの主要なデバイスプラットフォームをすべてサポートし、そのすべてのデバイスでブラウザを幅広くサポートします。

SaaS アプリケーションとローカルアプリケーションの両方を対象にしたフェデレーテッドシングルサインオン

複数パスワードの必要性をなくし、パスワードの再利用といった不適切なセキュリティプラクティスを防ぎます。SMA では、クラウドでホストされる SaaS アプリケーションとキャンパスでホストされるアプリケーションのいずれにおいてもフェデレーテッド SSO を利用できます。SMA は、多くの認証サーバー、許可サーバー、アカウンティングサーバーや、業界をリードする多要素認証テクノロジーと統合することで、セキュリティを強化しています。セキュアな SSO は、SMA がエンドポイントの正常性ステータスとコンプライアンスのチェックを済ませた、許可されたエンドポイントデバイスのみで利用できます。アクセスポリシーエンジンにより、許可されたアプリケーションだけがユーザーに表示され、認証の成功後にアクセスが許可されます。このソリューションでは、VPN クライアントの使用時にもフェデレーテッド SSO がサポートされ、お客様はクライアントベースまたはクライアントレスのどちらのセキュアアクセスを使用する場合でも、シームレスな認証エクスペリエンスを得ることができます。

セキュリティ侵害と高度な脅威の阻止

SonicWall SMA はアクセスセキュリティの層を追加してセキュリティ体制を強化し、脅威の対象領域を減らします。

- SonicWall Capture ATP のクラウドベースのマルチエンジンサンドボックスとの統合を通じて、SMA は、管理されていないエンドポイントでユーザーがアップロードしたファイルや、企業ネットワークの外部からユーザーがアップロードしたファイルをすべてスキャンします。これにより、ランサムウェアやゼロデイマルウェアなどの高度な脅威に対して、ユーザーはオフィス内にいるときと同レベルの保護を外出中でも確保できます [1]。
- SonicWall Web アプリケーションファイアウォールサービスは、Web ベースの社内アプリケーションを保護する、十分に統合された低コストのソリューションを企業に提供します。これにより、悪意のあるユーザーアクセスや不正認証によるユーザーアクセスが行われた場合でも、データの機密性は確保され、社内の Web サービスへの侵入は阻止されます。
- Geo-IP/ ボットネット検出は、DDoS 攻撃やゾンビ攻撃から組織を守り、侵害されたエンドポイントがボットネットとして機能するのを防ぎます。

シームレスでセキュアな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」の性質により、管理者は、リモートアクセスで使用するコンピューターにファットクライアントのコンポーネントを手動でインストールする必要がなくなります。その結果、Java への依存と IT のオーバーヘッドが除去されるため、リモートアクセスの概念が大幅に拡大します。すなわち、プリインストールや事前構成が不要になるため、許可されたリモートワーカーは、世界中のどこからでも任意のコンピューターを使用して企業リソースに安全にアクセスできるようになります。セキュアなアクセスの最も純粋な形とは、統合されたシームレスなユーザーエクスペリエンスを提供する、HTML5 による完全なブラウザベースのものです。

「Always On (常に有効)」のエクスペリエンスの実現

シームレスなユーザーエクスペリエンスのために、SMA は管理対象の Windows デバイスに Always On VPN (常に有効な VPN) を提供します。管理者は、許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または信頼できないネットワークを検出すると常に VPN 接続を自動的に確立するよう設定を構成できます。Windows デバイスへの単一のログインイベントによって、企業リソースに対するセキュアな接続がユーザーにもたらされます。ユーザーが各自の VPN クライアントにログインしたり、追加のパスワードを維持したりする必要はありません。これにより、モバイルユーザーには、オフィスにいるときと同じようにミッションクリティカルなリソースにアクセスできるようなシームレスなエクスペリエンスがもたらされ、IT 管理者は、管理対象のデバイスへの制御を維持できるようになり、組織のセキュリティ体制が向上します。

直感的な管理と包括的なレポート機能

SonicWall が提供する Web ベースの直感的な管理プラットフォームである Central Management Server (CMS) は、アプライアンスの管理を効率化し、広範なレポート機能を提供します。使いやすい GUI により、個別または複数のアプライアンスとポリシーを明確に管理できます。各ページには、管理下にあるすべてのマシンの設定内容が表示されます。ポリシーの一元管理により、アクセスポリシーと構成の作成および監視が促進されます。ユーザー、デバイス、アプリケーションからデータ、サーバー、ネットワークへのアクセスを 1 つのポリシーで制御できます。IT 部門は定型業務を自動化し、アクティビティをスケジュールすることで、セキュリティチームを反復作業から開放して、インシデント対応などの戦略的なセキュリティ業務に専念させることができます。使いやすいレポートと一元化されたログにより、IT 部門は、ユーザーアクセスの傾向とシステム全体の正常性について洞察を引き出します。

24 時間利用可能なサービスの提供

組織は、サービスを維持し、高い信頼性で運用を継続することで、ミッションクリティカルなアプリケーションへのセキュアなアクセスを常に提供することが求められています。SMA アプライアンスは、単一のデータセンターを擁する組織では従来型のアクティブ / パッシブの高可用性 (HA) をサポートし、ローカルまたは分散型のデータセンターを擁する組織ではアクティブ / アクティブまたはアクティブ / スタンバイクラスタリングのグローバル HA をサポートします。どちらの HA モデルも影響を与えないフェイルオーバとセッションの持続性により、シームレスなユーザーエクスペリエンスを実現します。

標準装備のロードバランサーによる先行投資コストの削減

SMA アプライアンスに組み込まれた負荷分散機能により、中規模企業やエンタープライズでの導入で要求される拡張性のレベルが実現します。SMA アプライアンスの特定モデルは動的な負荷分散機能を提供し、需要に基づくインテリジェントなセッション負荷の割り当てとユーザーライセンスの配分をリアルタイムで行います。組織は外部のロードバランサーに投資する必要がないため、先行投資コストが削減されます。

予期せぬイベントに備えた保険の確保

完全な事業継続と災害復旧ソリューションでは、セキュリティとコスト管理を維持しながら、リモートアクセスのトラフィック急増に対処できなければなりません。SMA の SonicWall スパイクライセンスパックは、分散型の企業が最大容量に達するまでユーザー数を瞬時に増やすことでシームレスな事業継続を可能にするアドオンライセンスです。スパイクライセンスは、将来における計画済み / 計画外の現行ユーザー数の急増 (数十から数百もの追加ユーザー) に備える保険契約のように機能します。

ニーズに合った VPN クライアントの導入

さまざまな VPN クライアントの中から、ノートパソコン、スマートフォン、タブレットなどの各種エンドポイントに対する、ポリシー適用のセキュアなリモートアクセスを実現するものを選ぶことができます。

VPN クライアント	サポートされる OS	サポートされる SMA モデル	要点
Mobile Connect	iOS、OS X、Android、Chrome OS、Windows 10	すべてのモデル	生体認証、アプリごとの VPN、エンドポイント制御の実施
Connect Tunnel (シンクライアント)	Windows、Mac OS、Linux	6200、6210、7200、7210、8200v、9000	堅牢なエンドポイント制御で完全な「オフィス内」体験を実現
NetExtender (シンクライアント)	Windows、Linux	210、410、500v	きめ細かいアクセスポリシーを適用し、ネイティブクライアントでネットワークアクセスを拡張

高度な認証

フェデレーテッドシングルサインオン [2]	SMA は SAML 2.0 認証を使用して、オンプレミスとクラウドのいずれのリソースに対しても単一ポータルを介したフェデレーテッド SSO が可能になり、セキュリティ強化のために多要素のスタック認証が実施されます。
多要素認証	X.509 デジタル証明書 サーバーサイド / クライアントサイドのデジタル証明書 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 Common Access Card (CAC) デュアル認証 / スタック認証 Captcha のサポート、ユーザー名 / パスワード
SAML 認証	SMA を SAML Identity Provider (IdP)、SAML Service Provider (SP)、または既存のオンプレミス IdP 上のプロキシとして構成し、SAML 2.0 認証を使用してフェデレーテッドシングルサインオン (SSO) を可能にすることができます。
認証リポジトリ	業界標準のリポジトリとのシンプルな統合により、ユーザーアカウントとパスワードを容易に管理できます。 RADIUS、LDAP、または Active Directory 認証リポジトリに基づいて、ネストされたグループを含むユーザーグループを動的に取り込むことができます。 共通またはカスタムの LDAP 属性を調べて、特定の権限やデバイスの登録を確認できます。
レイヤ 3 ～ 7 のアプリケーションプロキシ	SMA は、柔軟なプロキシオプションを備えています。たとえば、ベンダーのアクセスは直接プロキシで提供し、請負業者のアクセスはリバースプロキシで提供し、従業員は ActiveSync を介して Exchange にアクセスできます。
リバースプロキシ	拡張されたリバースプロキシサービスの認証により、管理者はアプリケーションオフロードポータル / ブックマークを構成できます。ユーザーは、RDP、HTTP などのリモートアプリケーション / リソースにシームレスに接続できます。この機能は、IE、Chrome、Firefox をはじめとするすべてのブラウザをサポートします。
Kerberos 制約付き委任	SMA は既存の Kerberos インフラストラクチャを使用した認証をサポートしており、フロントエンドサービスを信頼してサービスを委任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を許可または拒否し、セッション隔離時の修復措置を設定します。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、ID、デバイス、アプリケーション、データ、時間の要素が使用されます。
エンドポイント制御 (EPC)	EPC を使用すると、管理者は接続デバイスの正常性ステータスに基づいて、きめ細かいアクセス制御ルールを実施できます。OS との緊密な統合により、多くの要素を組み合わせたタイプ分類とリスク要因評価が行われます。EPC のチェックによって、デバイスプロファイルのセットアップが簡素化されます。これには、Windows、Mac、Linux プラットフォームのアンチウイルス、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定義済みリストが使用されます。このリストには、シグネチャファイル更新のバージョンと適用範囲が含まれます。
アプリアクセス制御 (AAC)	管理者は、個々のアプリケーショントンネルを通じて、特定のモバイルアプリケーションがアクセス可能なネットワーク上のリソースを定義できます。AAC のポリシーはクライアントとサーバーの両方に適用されるため、堅牢な境界の保護が実現します。

優れたセキュリティ

レイヤ 3 SSL VPN	SMA シリーズは、さまざまな環境で実行される各種のクライアントデバイスに高性能なレイヤ 3 トンネリング機能を提供します。
暗号化のサポート	セッションの長さを設定可能 暗号：AES 128 + 256 ビット、トリプル DES、RC4 128 ビット ハッシュ：SHA-256 ECDSA (楕円曲線デジタル署名アルゴリズム)
高度な暗号のサポート	SMA アプライアンスでは、すぐに使用できるデフォルト設定の暗号により、コンプライアンスを満たす強力なセキュリティ体制を実現します。管理者は、パフォーマンスやセキュリティの強度、互換性をきめ細かく調整できます。
セキュリティ認定	FIPS 140-2 レベル 2、ICSA SSL-TLS の認定、Common Criteria と UC-APL は認証中
セキュアなファイル共有 [1]	自動修復機能により、ランサムウェアなどの未知のゼロデイ攻撃をゲートウェイで阻止します。管理されていないエンドポイントからセキュアなアクセスでアップロードされた、企業ネットワークへのファイルは、クラウドベースのマルチエンジン Capture ATP で検査されます。
Web アプリケーション ファイアウォール (WAF)	プロトコル /Web ベースの攻撃を防ぎ、金融、ヘルスケア、e コマースなどの企業が OWASP Top 10 と PCI 準拠を達成できるように支援します。
Geo IP 検出とボットネット対策	Geo IP 検出とボットネット対策により、さまざまな地理的場所からのユーザーアクセスを許可または制限するメカニズムを利用できます。

直感的なユーザーエクスペリエンス

Always On VPN (常に有効な VPN)	企業提供の Windows デバイスから企業ネットワークへのセキュアな接続を自動的に確立して、セキュリティを向上し、トラフィックを可視化し、コンプライアンスへの準拠を維持します。
セキュアネットワーク検出 (SND)	SMA のネットワーク対応 VPN クライアントは、デバイスがキャンパス外にある場合はこれを検出し、VPN を自動再接続して、デバイスが信頼できるネットワークに戻ると VPN を再度停止します。
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 の各プロトコルを提供する HTML5 ブラウザエージェントを介して、リソースへのセキュアなクライアントレスアクセスを実現します。
シングルサインオンのポータル	WorkPlace ポータルでは、使いやすいカスタマイズ可能な単一ビューにより、ハイブリッドな IT 環境のリソースに対する、シングルサインオン (SSO) を使用したセキュアなアクセスを可視化できます。追加のログインや VPN は不要です。
レイヤ 3 トンネリング	管理者はスプリットトンネルモードを選択するか、リダイレクトオールモードを実行できます。リダイレクトオールモードでは SSL/TLS トンネリングが使用され、オプションの ESP フォールバックで最大のパフォーマンスが得られます。
HTML5 ファイルエクスプローラ [1]	最新のファイルブラウザにより、ユーザーは任意の Web ブラウザからファイル共有に容易にアクセスできます。
モバイル OS との統合	Mobile Connect はすべての OS プラットフォームでサポートされているため、ユーザーはモバイルデバイスを自由に選択できます。

弾力性

グローバルトラフィック オプティマイザ (GTO)	SMA は、ユーザーに影響を与えないグローバルなトラフィック負荷分散を実現します。トラフィックは、最もパフォーマンスが高い最適なデータセンターに送られます。
動的な高可用性 [2]	SMA はアクティブ / パッシブ構成をサポートし、高可用性を実現するアクティブ / アクティブ構成を備えています。この構成は単一のデータセンターに導入することも、地理的に分散している複数のデータセンターに導入することもできます。
ユニバーサルなセッション持続性 [1]	影響を与えないフェイルオーバにより、シームレスなユーザーエクスペリエンスを実現します。アプライアンスがオフラインになった場合でも、SMA のインテリジェントクラスタリングにより、ユーザーは再認証を必要とせずにそのセッションデータとともに再配分されます。
拡張が容易なパフォーマンス	SMA アプライアンスは、複数のアプライアンスの配置によってパフォーマンスを飛躍的に拡張でき、単一障害点が排除されます。水平クラスタリングにより、物理 / 仮想の SMA アプライアンスの混在使用を完全にサポートします。
動的なライセンス	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がなくなります。ユーザーの需要に基づいて、管理対象のアプライアンス間でユーザーを動的に配分および再配分できます。

中央管理 / 監視

中央管理システム (CMS)	CMS を使用すると、SMA のすべての機能を Web で一元管理できます。
カスタムアラート	SNMP トラップを生成するようにアラートを構成できます。このトラップは、任意の IT インフラストラクチャの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 ファイルスキャンのアラートや、即時アクションのためのディスク使用量も構成できます。
リアルタイムダッシュボード	リアルタイムで、カスタマイズ可能なダッシュボードを使用すると、IT 管理者はアクセスの問題を迅速かつ容易に診断して、トラブルシューティングの有益な洞察を得ることができます。
SIEM 統合	中央の SIEM データコレクターへのリアルタイム出力により、セキュリティチームは、イベントドリブンのアクティビティを関連付けて、特定のユーザーや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できます。これは、セキュリティインシデント管理やフォレンジック分析に欠かせないものです。
スケジューラ	スケジューラを使用すると、ユーザーはポリシーの導入、構成設定の複製、サービスの再開などの保守作業をスケジュールして、手動による介入なしで実行できます。

拡張性

管理 API	管理 API により、1 つの SMA または グローバルな CMS 環境のすべてのオブジェクトに対するプログラムをフルに使用した管理が実現します。
エンドユーザー API	エンドユーザー API は、すべてのログオン、認証、エンドポイントのワークフローを完全に制御します
二要素認証 (2FA)	SMA は、Google Authenticator、Microsoft Authenticator、Duo security など業界トップクラスの Time-based One-Time Password (TOTP) ソリューションを統合することで 2FA を実現します。
MDM 統合	SMA は、Airwatch、Mobile Iron などの主要なエンタープライズモバイル管理 (EMM) 製品と統合されます。
その他のサードパーティ製品との統合	SMA は OPSWAT などの業界をリードするベンダーと統合し、高度な脅威防御を実現します。

[1] SMA OS 12.1 以降で利用可能

[2] SMA 12.1 で拡張

機能の要約 (モデル別の比較)

カテゴリ	機能	210	410	500v	6210	7210	8200v
スループット	最大同時ユーザーセッション	50	250	250	2,000	10,000	5,000
	最大 SSL/TLS スループット	560 Mbps	844 Mbps	186 Mbps	400 Mbps	3.75 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 / リダイレクトオール	●	●	●	●	●	●
	Always On VPN (常に有効な 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出	–	–	–	●	●	●
	ファイルブラウザ (CIFS/NFS)	●	●	●	●	●	●
	Citrix XenDesktop/XenApp	●	●	●	●	●	●
	VMware View	–	–	–	●	●	●
	オンデマンドトンネル	–	–	–	●	●	●
	Chrome/Firefox の拡張機能	–	–	–	●	●	●
	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	アプリごとの VPN	–	–	–	●	●	●
	アプリ制御の実施	–	–	–	●	●	●
	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	–	–	–	●	●	●
	ローカライズ	●	●	●	●	●	●
	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	–	–	–	●	●	●
	スイート B 暗号	–	–	–	●	●	●
	動的な EPC 調査	●	●	●	●	●	●
	ロールベースのアクセス制御 (RBAC)	–	–	–	●	●	●
	エンドポイント登録	●	●	●	●	●	●
	セキュアなファイル共有 (Capture ATP)	●	●	●	●	●	●
	エンドポイント隔離	●	●	●	●	●	●
	OSCP CRL 検証	–	–	–	●	●	●
	暗号の選択	–	–	–	●	●	●
	PKI およびクライアント証明書	●	●	●	●	●	●
	Geo IP フィルター	●	●	●	–	–	–
	ボットネットフィルター	●	●	●	–	–	–
	フォワードプロキシ	●	●	●	●	●	●
	リバースプロキシ	●	●	●	●	●	●
認証と ID サービス	SAML 2.0	–	–	–	●	●	●
	LDAP、RADIUS	●	●	●	●	●	●
	Kerberos (KDC)	●	●	●	●	●	●
	NTLM	●	●	●	●	●	●
	SAML Identity Provider (IdP)	–	–	–	●	●	●
	バイオメトリックデバイスのサポート	●	●	●	●	●	●
	iOS に対する Face ID サポート	●	●	●	●	●	●
	二要素認証 (2FA)	●	●	●	●	●	●
	多要素認証 (MFA)	–	–	–	●	●	●

機能の要約 (モデル別の比較)

カテゴリ	機能	210	410	500v	6210	7210	8200v
認証と ID サービス (続き)	チェーン認証	–	–	–	●	●	●
	電子メールまたは SMS 経由の One Time Passcode (OTP)	●	●	●	●	●	●
	Common Access Card (CAC) のサポート	–	–	–	●	●	●
	X.509 認証サポート	●	●	●	●	●	●
	Captcha 統合	–	–	–	●	●	●
	リモートでのパスワード変更	●	●	●	●	●	●
	フォームベース SSO	●	●	●	●	●	●
	フェデレーテッド SSO	–	–	–	●	●	●
	セッションの持続性	–	–	–	●	●	●
	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 (イーサネット)	–	–	–	●	●	●
	管理インターフェイス (コンソール)	–	–	–	●	●	●
	HTTPS 管理	●	●	●	●	●	●
	SSH 管理	–	–	–	●	●	●
	SNMP MIBS	●	●	●	●	●	●
	Syslog および NTP	●	●	●	●	●	●
	使用状況監視	●	●	●	●	●	●
	構成のロールバック	●	●	●	●	●	●
	一元管理	–	–	–	●	●	●
	一元化されたレポート	–	–	–	●	●	●
	管理 REST API	–	–	–	●	●	●
	認証 REST API	–	–	–	●	●	●
	RADIUS アカウント	–	–	–	●	●	●
	スケジュールタスク	–	–	–	●	●	●
	一元化されたセッションライセンス	–	–	–	●	●	●
	イベントドリブンの監査	–	–	–	●	●	●
ネットワーク	IPv6	●	●	●	●	●	●
	グローバルな負荷分散	–	–	–	●	●	●
	サーバーの負荷分散	●	●	●	–	–	–
	TCP 状態の複製	●	●	●	●	●	●
	クラスタ状態のフェイルオーバ	–	–	–	●	●	●
	アクティブ / パッシブの高可用性	–	●	●	●	●	●
	アクティブ / アクティブの高可用性	–	–	–	●	●	●
	水平方向の拡張性	–	–	–	●	●	●
	単一または複数の FQDN	–	–	–	●	●	●
	L3-7 スマートトンネルプロキシ	●	●	●	●	●	●
	L7 アプリケーションプロキシ	●	●	●	●	●	●
統合	2FA TOTP のサポート	●	●	●	●	●	●
	EMM/MDM 製品サポート	–	–	–	●	●	●
	SIEM 製品サポート	–	–	–	●	●	●
	TPAM パスワードボールト	–	–	–	●	●	●
	ESX ハイパーバイザーのサポート	–	–	●	–	–	–
	Hyper-V ハイパーバイザーのサポート	–	–	●	–	–	–
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	–	–	–	●	●	●
	無期限ライセンス (サポートが必要)	●	●	●	●	●	●
	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	●	●	●	●	●	●
	階層型ライセンス	–	–	–	●	●	●
	仮想アシスト	●	●	●	–	–	–

* VPN クライアントの詳細については、当社の Web サイトをご覧ください。https://www.sonicwall.com/en-us/products/remote-access/vpn-client

ハイエンドアプライアンスへのアップグレードがもたらすメリット

パフォーマンスの向上 | スループットの増加 | 高度な機能 | 拡張性の向上

アプライアンスの仕様

さまざまな用途に応じた Secure Mobile Access (SMA) アプライアンスの中からお選びください。
仮想 / 物理アプライアンスの柔軟な導入オプションをご利用いただけます。

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	最大 50	最大 250	最大 2,000	最大 10,000
SSL VPN スループット * (最大 CCU 時)	560 Mbps	844 Mbps	最大 400 Mbps	最大 3.75 Gbps
フォームファクタ	1U	1U	1U	1U
寸法	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 (16.92 x 10.23 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 (17.0 x 16.5 x 1.75 インチ)
アプライアンスの重量	5 kg (11 ポンド)	5 kg (11 ポンド)	8 kg (17.7 ポンド)	8.3 kg (18.3 ポンド)
暗号化データアクセラレーション (AES-NI)	なし	なし	あり	あり
専用の管理ポート	なし	なし	あり	あり
SSL アクセラレーション	なし	なし	あり	あり
ストレージ	4GB (フラッシュメモリ)	4GB (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 イーサネット、(2) USB、(1) コンソール	(4) GB イーサネット、(2) USB、(1) コンソール	(6) ポート 1GE、(2) USB、(1) コンソール	(6) ポート 1GE、(2) ポート 10Gb SFP+、(2) USB、(1) コンソール
メモリ	4 GB	8 GB	8 GB DDR4	16GB DDR4
TPM チップ	なし	なし	あり	あり
プロセッサー	4 コア	8 コア	4 コア	4 コア
MTBF (25° C/77° F)	61,815 時間	60,151 時間	70,127 時間	129,601 時間
運用とコンプライアンス	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
電源	固定電源	固定電源	固定電源	デュアル電源装置、ホットスワップ対応
入力定格	100 ～ 240 VAC、50 ～ 60 MHz	100 ～ 240 VAC、50 ～ 60 MHz	100 ～ 240 VAC、1.1 A	100 ～ 240 VAC、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	WEEE、EU RoHS、中国 RoHS			
非動作時最大衝撃	110 g、2 ミリ秒			
排出	FCC、ICES、CE、C-Tick、VCCI、MIC			
安全性	TUV/GS、UL、CE PSB、CCC、BSMI、CB スキーム			
作動時温度	0 ～ 40° C (32 ～ 104° F)			
FIPS 認定	なし	なし	FIPS 140-2 レベル 2、改ざん防止保護	

* スループットパフォーマンスは導入環境と接続条件によって異なる場合があります。記載されている数値は社内ラボの条件に基づいています。

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 時)	最大 186 Mbps	最大 1.58 Gbps
割り当てメモリ量	2 GB	8 GB
プロセッサー	1 コア	4 コア
SSL アクセラレーション	なし	あり
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	Hardened Linux
専用の管理ポート	なし	あり

* スループットパフォーマンスは導入環境と接続条件によって異なる場合があります。記載されている数値は社内ラボの条件に基づいています。Windows Server 2016 で SMA OS 12.1 を実行しているとき、SMA 8200v (Hyper-V) は 5000 同時セッションまで拡張でき、最大 1.58 Gbps SSL-VPN スループットを実現します。

パートナー イネーブルド サービス

SonicWall ソリューションの計画、導入、最適化に支援が必要ですか。SonicWallAdvanced Services Partner は、世界規模のプロフェッショナルサービスを提供するように訓練されています。詳細は www.sonicwall.com/PES をご覧ください。

当社について

創設後 27 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。SonicWall Capture Labs の研究が支える、当社の受賞歴のあるリアルタイム侵害検出および防御のソリューションは、世界の 215 以上もの国や地域で 100 万以上のネットワークとその電子メール、アプリケーション、およびデータを保護してきました。これらの組織において、セキュリティの不安を解消し、より効果的な組織運営をお手伝いしています。詳細は、www.sonicwall.com にアクセスするか、Twitter、LinkedIn、Facebook、Instagram で当社をフォローしてください。

SONICWALL®

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SecureMobileAccess-US-VG-604

SONICWALL®