SMA 1000 シリーズ

強力できめ細かいアクセス制御エンジンにより、すべてのリモート/モバイルワーカーに対して堅牢なアクセスセキュリティを提供

業界の課題

セキュリティの確立されたオフィスの外部でビジネスが行われるようになり、企業の機密リソースのアクセス管理が CISO にとって最大の関心事となっています。ゲスト、顧客、パートナー、従業員にポリシーベースのアクセスを提供する、インテリジェントなアクセス・セキュリティ・ソリューションが求められています。BYOD、クラウド、リモートワークなどのトレンドはそれぞれ独自の課題を生んでいますが、根本的な問題も残されています。

- 権限のないユーザーが企業のデータやアプリケーションにアクセス
- マルウェアに感染したデバイスが媒介となって企業のシステムに感染
- 業務に影響を与えずに各種のモバイルプラットフォーム間で信頼できるサービスを維持
- 安全でないパブリック Wi-Fi ネットワークで送信中の企業データの傍受
- 監査/規制要件への準拠

SonicWall ソリューション

SMA 1000 シリーズは、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 の概要

アクセス制御エンジン

SMA 1000 シリーズでは、ネットワークとクラウドの企業データおよびアプリケーションへのリモート/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。BYOD、フレックスタイム制、オフショア開発などのアジャイルな働き方を採用したいと考えている組織にとって、SMA はそのすべての中心となる実施ポイントとして機能します。

SMA のアクセス制御エンジンは、ユーザーやエンドポイント、アプリケーションから生じるリスクを評価してからデータアクセスを許可します。セッション隔離やアラートなどの修復措置を実施して、ユーザーのフラストレーションを最小限に抑え、ヘルプデスクコールの回数を減らします。

安全なアクセス

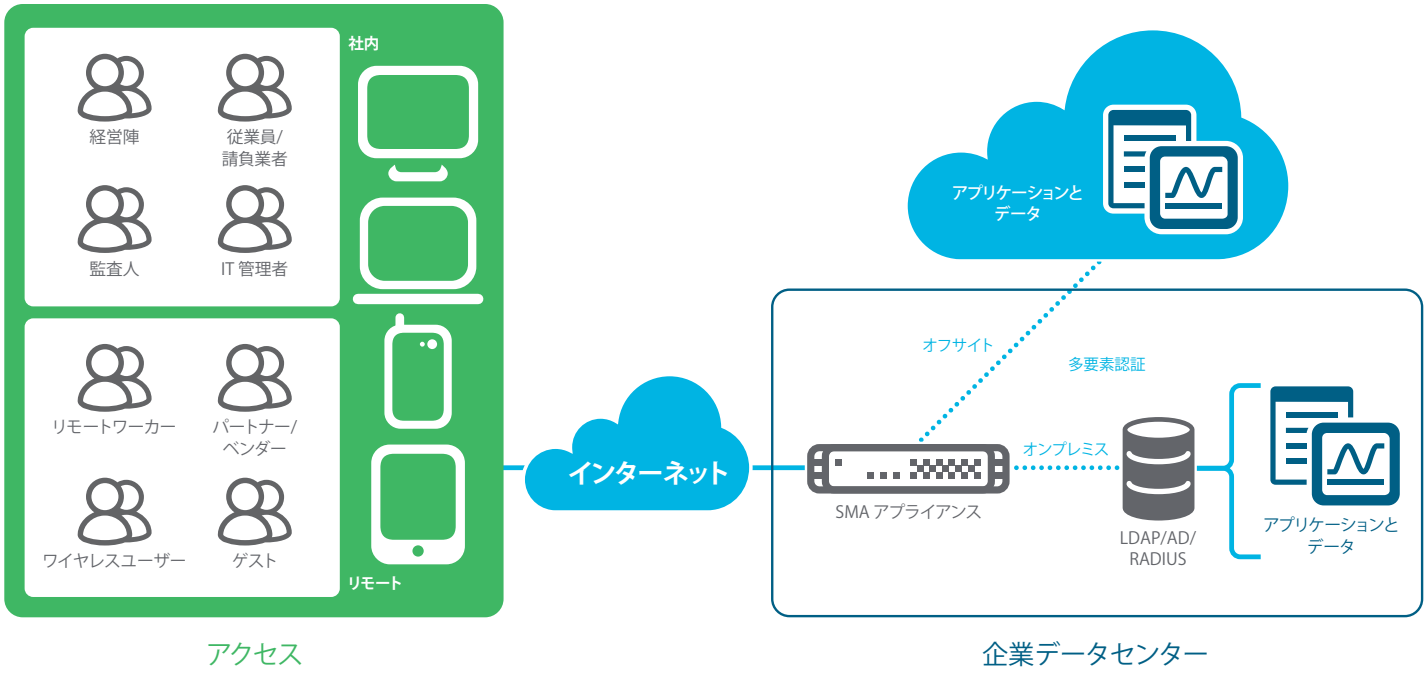
SMA 1000 シリーズは、直感的なクライアントにより、ユーザーの生産性向上に欠かせないファイル、アプリケーション、リソースへの安全なリモートアクセスを可能にします。このクライアントは、Windows、Mac OSX、Linux、iOS、Android、Chrome OS、Windows Mobile、Kindle Fire の各デバイスへ容易に導入できます。SMA はクラス最高のセキュリティを実現して既知の脅威を最小化し、最新の暗号化アルゴリズムをサポートすることで組織のセキュリティを強化します。

クライアント不要のアクセスセキュリティ

SMA OS 12 HTML5 アプリケーションエージェントは、使用頻度が最も高いデータタイプへの安全なアクセス手段を提供し、悪意のある攻撃やマルウェアの増殖を防ぎます。これらの多機能なエージェントは、ネイティブアプリケーションと同等に機能します、これは、ユーザーエクスペリエンスの向上に欠かせないことです。クライアント不要のセキュリティによって即日のデバイスサポートが実現し、インストールが不要なためフットプリントがゼロになり、サードパーティや管理されていないエンドポイントからのアクセスに最適です。

メリット:

- きめ細かいアクセス制御エンジンにより、誰にどのリソースへのアクセス権を与えるかを定義
- Advanced Endpoint Control モジュールにより、すべての接続デバイスを調べて、エンドポイントの正常性に基づいてアクセスを許可または拒否
- グローバル高可用性プラットフォームによってトラフィックを最適化し、パフォーマンスに影響しないフェイルオーバを実現
- 最新の暗号技術を活用することで、データ保護と優れたセキュリティを実現
- 包括的な監査証跡によって規制準拠を支援



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。

アクセス管理

エンドポイントとエッジでの継続的なアクセス実施が、企業データの損失と盗難の防止に役立ちます。SMA は、堅牢できめ細かいポリシー管理エンジンを通じて、データの機密性と完全性を確保します。SMA は、ネットワークに入る前にすべてのユーザー、エンドポイント、アプリケーションを検証することで、データを保護してユーザーの処理能力を高めます。

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

利用可能な最新の暗号技術と最強の暗号化手法を活用することで、SMA は、コンプライアンスとデータ保護を実現する最高水準のセキュリティ体制を維持します。すべてのハードウェアモデルを業界の厳格なセキュリティのテストと認定に従っているかどうか定期的に確認することで、SonicWall は政府機関や医療/金融業界の規制要件をサポートします。

レイヤ 3 SSL VPN	SMA 1000 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: MD5、SHA-256、SHA-1 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 1000 ソリューションでは、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

グローバル高可用性

SMA 1000 シリーズは、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。グローバル高可用性（GHA）により、サービス所有者は一連のツールを使用してダウンタイムなしでサービスを提供し、厳格な SLA を達成できます。

SonicWall 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	SMA OS 12 は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おり、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。
拡張が容易なパフォーマンス	SMA 1000 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。

SONICWALL™

中央管理/監視

SMA は、アプライアンス管理を効率化する、多彩なレポート機能を備えた Web ベースの管理プラットフォームを提供します。

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。
SONAR 監視	SonicWall SONAR 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の実行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

SMA の拡張性プログラムは、当社の製品を補完的なセキュリティソリューションと結びつけ、業界リーダーとの統合や強力な API の提供によって顧客、パートナー、サードパーティの能力を高めます。

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関して、プログラムを使用した完全な管理が実現します。
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。
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。

高度な認証

SMA 1000 シリーズは、シンプルで一貫性のあるユーザーエクスペリエンスをシングルサインオン（SSO）で実現し、脅威の実行者や資格情報の収奪から組織を防御します。

クラウドのシングルサインオン	SMA SAML IdP プロキシにより、従来の AD のユーザー名/パスワードと SaaS クラウドリソースのいずれに対しても単一ポータルを介した 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、Defender およびその他のワンタイムパスワード/2 要素認証トークン（RADIUS プロトコルを使用） 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 Gatekeeper のサポート	FIPS 認定のエッジ・ポイント・アプライアンスの資格情報チェーン技術により、キャンパスでホストされる SAML IdP にエアギャップセキュリティを提供します。
認証リポジトリ	業界標準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。例えば、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。
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。

直感的なユーザーエクスペリエンス

好ましいユーザーエクスペリエンスは、最強のセキュリティポリシーの採用をユーザーに促し、データ損失の深刻なリスクをもたらすシャドー IT シナリオを防止します。

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安全なクライアントレスアクセスを実現します。
ユーザーポータル	WorkPlace ポータルでは、リソースが動的にパーソナライズされた、カスタマイズ可能の直感的なランディングページを利用できます。
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。後者のモードでは 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。
セッションの持続性	SMA は、再認証を必要とせずに異なる場所でのセッションの持続性を確保します。
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。

機能の要約

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
- 自動 ESP カプセル化
- HTML5（RDP/VNC/ICA/SSH）
- 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・ブラウザ・トンネル
- Chrome/Firefox の拡張機能
- CLI トンネルのサポート
- マルチクライアント OS

モバイル

- 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
- エンドポイント登録
- 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
- フォワードプロキシ

認証

- LDAP、RADIUS
- Kerberos（KDC）
- NTLM
- SAML IdP ゲートキーパー
- バイオメトリックデバイスのサポート
- チェーン認証
- リモートでのパスワード変更
- フォームベース SSO
- チーム ID セッションの持続性
- 自動ログオン
- リバースプロキシ

アクセス制御

- グループ AD
- LDAP 属性
- 継続的な監視

管理

- 専用 OOB（シリアル/イーサネット）
- グローバルな負荷分散
- 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/アクティブの高可用性
- 水平クラスタリングの拡張性
- 一元管理
- デバイスの HTTPS および SSH の管理
- SNMP MIBS
- Syslog および NTP
- 構成のロールバック
- バーストライセンス
- 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
- 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
- 一元化されたレポート

統合

- 管理 REST API
- 認証 REST API
- TPAM パスワードボールト
- EMM/MDM 製品サポート
- SIEM 製品サポート

ライセンスオプション

- サブスクリプション（サポートを含む）
- 無期限（サポートが必要）

ハードウェアアプライアンス

SMA 6200/7200

SRA EX9000

パフォーマンス	SMA 6200	SMA 7200	SRA EX9000
同時セッション/ユーザー	最大 2,500	最大 10,000	最大 20,000
SSL VPN スループット（最大 CCU 時）	最大 400 Mbps	最大 3.75 Gbps	最大 3.75 Gbps
特性	**SMA 6200**	**SMA 7200**	**SRA EX9000**
フォームファクタ	1U	1U	2U
寸法	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）	68.6 x 48.2 x 8.8 cm（27.0 x 18.9 x 3.4 インチ）
データ暗号化アクセラレーション（AES-NI）	あり	あり	あり
専用の管理ポート	あり	あり	あり
SSL アクセラレーション	あり	あり	あり
ハードドライブ	2 x 500 GB SATA	2 x 500 GB SATA	2 x 2TB SATA
インターフェイス	6（6 ポート 1GE）	8（6 ポート 1GE + 2 ポート 10Gb SFP+）	12（8 ポート 1GE + 4 ポート 10Gb SFP+）
メモリ	8 GB DDR3	16 GB DDR3	32 GB DDR3
TPM チップ	あり	あり	なし
プロセッサー	4 コア	4 コア	2 x 4 コア
MTBF	200,064 時間（25°C/77°F）	233,892 時間（25°C/77°F）	129,489 時間（25°C/77°F）
運用とコンプライアンス	**SMA 6200**	**SMA 7200**	**SRA EX9000**
電源	固定電源	デュアル電源装置、ホットスワップ対応	デュアル電源装置、ホットスワップ対応
入力定格	100～240 VAC、1.1 A	100～240 VAC、1.79 A	100～240 VAC、2.85 A
消費電力	78 W	127 W	320 W
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）		
認定	FIPS 140-2 レベル 2、改ざん防止保護		

仮想アプライアンスの仕様

	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper V)
同時セッション	最大 5000	最大 250
SSL VPN スループット (最大 CCU 時)	最大 1.58 Gbps	最大 1.2 Gbps
割り当てメモリ量	8 GB	
プロセッサー	4 コア	
SSL アクセラレーション	あり	
適用ディスクサイズ	64 GB (デフォルト)	管理者が設定可能
インストール済みオペレーティングシステム	Hardened Linux	
専用の管理ポート	あり	

コア SKU

SMA アプライアンス	SKU 番号
SMA 8200v	01-SSC-8468
SMA 6200	01-SSC-2300
SMA 7200	01-SSC-2301
SRA EX9000	01-SSC-9574
50 ユーザー CCU	01-SSC-7859
250 ユーザー CCU	01-SSC-7861
1,000 ユーザー CCU	01-SSC-7863
250 ユーザー 3 年サポート	01-SSC-2331
1,000 ユーザー 3 年サポート	01-SSC-2337

オプション SKU

SMA アドオン	SKU 番号
CMS ベース (最大 3 アプライアンス)	01-SSC-8535
CMS 最大 100 アプライアンス 1 年間	01-SSC-8536
50 ユーザープールライセンス*	01-SSC-2401
250 ユーザープールライセンス*	01-SSC-2403
1,000 ユーザープールライセンス*	01-SSC-8539
SMA 7200 用 FIPS アドオン	01-SSC-2406
SMA 6200 用 FIPS アドオン	01-SSC-2405
SMA 6200 用 10 日 5〜1000 スパイク	01-SSC-2368

**プールライセンスには GTO および SONAR が含まれます。*

当社について

創設後 25 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。ネットワークセキュリティから、アクセスセキュリティ、E メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SMA-1000Series-US-KJ-24735

SONICWALL™