SonicWall SuperMassive シリーズ

企業ネットワークを保護する、妥協のない高性能な次世代ファイアウォール

SonicWall SuperMassive シリーズは、大規模なネットワーク向けに設計された SonicWall の次世代ファイアウォール（NGFW）プラットフォームです。拡張性、信頼性、高度なセキュリティ機能を備えており、ほとんど遅延のないマルチギガビットの速度で動作します。

企業、政府機関、大学、サービスプロバイダの導入ニーズを満たすように設計された SuperMassive シリーズは、企業ネットワーク、データセンター、サービスプロバイダのセキュリティ保護に最適です。

大規模なマルチコアアーキテクチャと、SonicWall の特許取得済み* Reassembly-Free Deep Packet Inspection®（RFDPI）（再構築不要のディープ・パケット・インスペクション）テクノロジーを組み合わせることで、SuperMassive E10000 シリーズおよび 9000 シリーズは、業界をリードするアプリケーションコントロール、侵入防止、マルウェア防御、SSL インスペクションをマルチギガビットの速度で実現します。SuperMassive シリーズは、電力、スペース、冷却（PSC: Power/Space/Cooling）を念頭に設計されており、アプリケーションコントロールと脅威防御において業界トップクラスの Gbps/ワットを誇る NGFW です。

SonicWall の RFDPI エンジンは、すべてのポートで全パケットの全バイトをスキャンし、高いパフォーマンスと低いレイテンシを維持しながら、ストリーム全体の完全なコンテンツ検査を実現します。このテクノロジーは、アンチマルウェアプログラムに組み込まれたソケットでコンテンツを再構築する旧式のプロキシ設計よりも優れています。コンテンツを再構築する設計は効率が悪く、ソケットメモリのスラッシングによるオーバーヘッドが発生し、高レイテンシ、低パフォーマンス、ファイルサイズの制限をもたらします。RFDPI エンジンは、脅威がネットワークに侵入する前に完全なコンテンツ検査を実施し、何百万種類にもおよぶ多様なマルウェアを防御します。その際、ファイルサイズやパフォーマンス、レイテンシは制限されません。さらに、RFDPI エンジンは SSL で暗号化されたトラフィックやプロキシ化できないアプリケーションに対しても完全な検査を実施できるため、トランスポートやプロトコルに関係なく包括的な保護が実現します。

アプリケーショントラフィックの分析により、そのトラフィックが生産的なものであるか、非生産的なものであるかをリアルタイムで識別し、強力なアプリケーションレベルのポリシーでトラフィックを制御できます。アプリケーションコントロールは、スケジュールや例外リストを併用して、ユーザー別またはグループ別に実施できます。アプリケーション、侵入防止、マルウェアのシグネチャはすべて SonicWall の脅威調査チームによって随時更新されています。さらに、先進的な専用のオペレーティングシステムである SonicOS は、カスタムアプリケーションを識別、制御する統合ツールを提供します。

SuperMassive シリーズのファイアウォール設計では、ほぼ直線的にパフォーマンスが向上し、処理能力を最大 96 コアまで拡張できます。これにより、最大で 40 Gbps のファイアウォールスループット、30 Gbps の脅威防御、30 Gbps のアプリケーションインスペクションおよびコントロールが可能になります。SuperMassive E10000 シリーズは現場でアップグレードできるため、ネットワーク帯域幅やセキュリティ要件が拡大しても、セキュリティインフラストラクチャへの投資が将来にわたって保証されます。

SuperMassive E10000 シリーズ

SuperMassive 9000 シリーズ

メリット:

- 高性能な侵入防止、低レイテンシのマルウェア対策、ネットワークサンドボックスを備えた包括的な脅威防御
- きめ細かい優れたアプリケーションインテリジェンス、コントロール、可視化
- ソケットベースの SSL プロキシに付随するオーバーヘッド、レイテンシ、メモリスラッシングを排除した、SSL 暗号化トラフィックの完全な検査
- 10/40 Gbps インフラストラクチャ用に設計された、大規模な拡張が可能なマルチコアアーキテクチャ

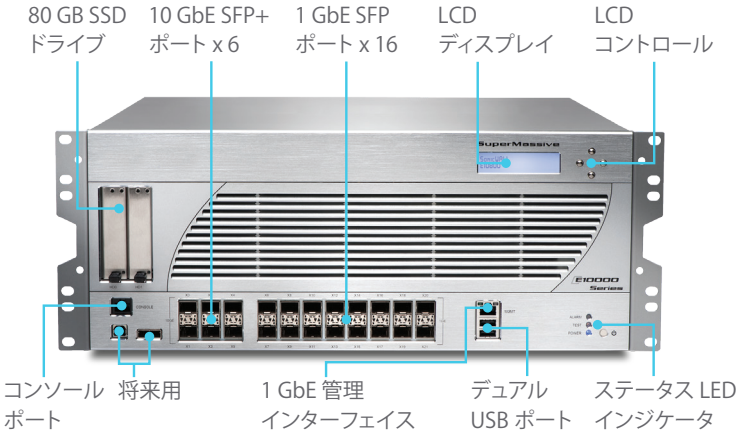
米国特許 7,310,815; 7,600,257; 7,738,380; 7,835,361

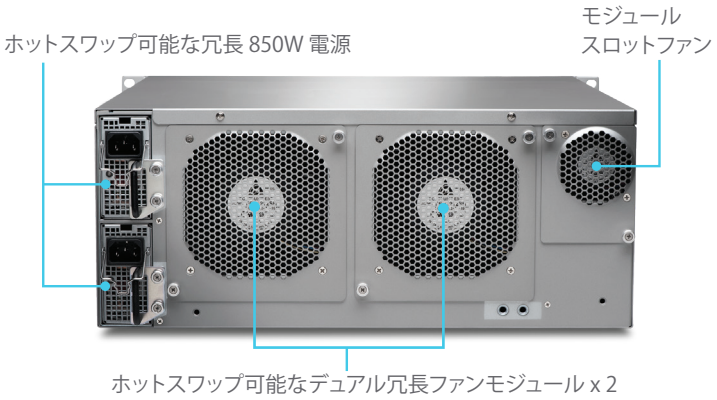
シリーズラインナップ

SonicWall SuperMassive E10000 シリーズの筐体は、10 GbE SFP+ x 6、1 GbE SFP ポート x 16、850 W の冗長 AC 電源、ホットスワップ可能なデュアル冗長ファンモジュールを備えており、最大 96 プロセッシングコアまでの大規模な拡張が可能です。

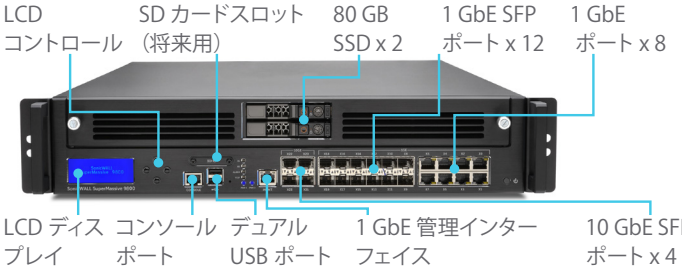
SonicWall SuperMassive 9000 シリーズは、10 GbE SFP+ x 4、1 GbE SFP x 12（最大）、1 GbE 銅線 x 8、1 GbE 管理インターフェイスのほか、10 GbE SFP+ インターフェイスを 2 基（今後のリリース）追加できる拡張ポートを備えています。9000 シリーズは、ホットスワップ可能なファンモジュールと電源を搭載しています。

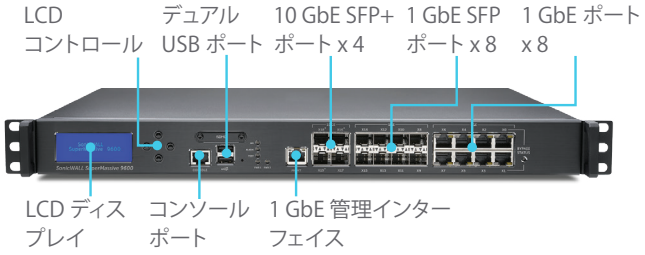
SuperMassive E10000 シリーズ





SuperMassive 9000 シリーズ



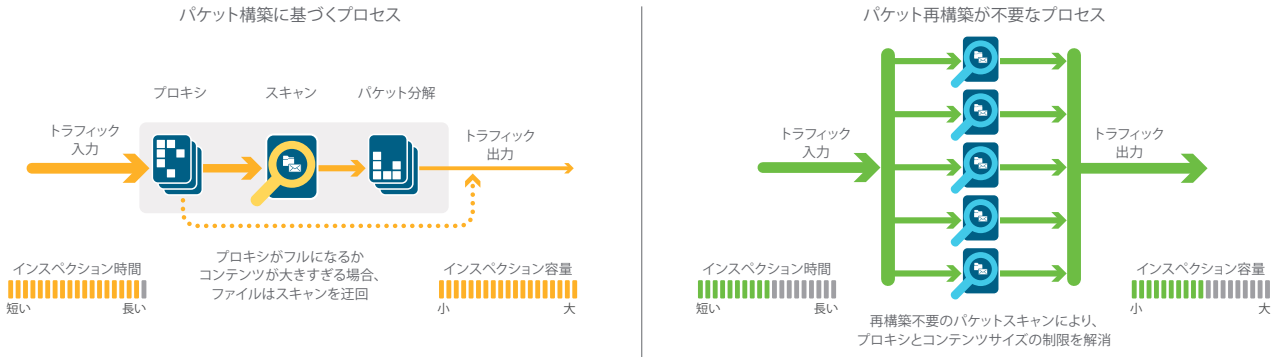


機能	9200	9400	9600	9800	E10400	E10800
プロセッシングコア	24	32	32	64	48	96
ファイアウォールのスループット	15 Gbps	20 Gbps	20 Gbps	40 Gbps	20 Gbps	40 Gbps
アプリケーションインテリジェンスのスループット	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	28 Gbps
侵入防止システム（IPS）のスループット	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps	15 Gbps	30 Gbps
アンチマルウェア	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps	6 Gbps	12 Gbps
最大 DPI 接続数	1.25 M	1.25 M	1.5 M	2.5 M	5 M	10 M
導入モード	**9200**	**9400**	**9600**	**9800**	**E10400**	**E10800**
L2 ブリッジモード	対応	対応	対応	対応	対応	対応
ワイヤモード	対応	対応	対応	対応	対応	対応
ゲートウェイ/NAT モード	対応	対応	対応	対応	対応	対応
タップモード	対応	対応	対応	対応	対応	対応
トランスペアレントモード	対応	対応	対応	対応	対応	対応

Reassembly-Free Deep Packet Inspection エンジン

RFDPI エンジンは、パフォーマンスを損なわずに優れた脅威防御とアプリケーションコントロールを実現します。この特許取得済みのエンジンは、ストリーミングトラフィックのペイロードを検査して、レイヤ 3〜7 の脅威を検出します。さらに、検出エンジンを混乱させて悪意のあるコードをネットワークに潜入させる高度な回避手法を無効にするために、ネットワークストリームで大規模な正規化と復号化を繰り返し実行します。

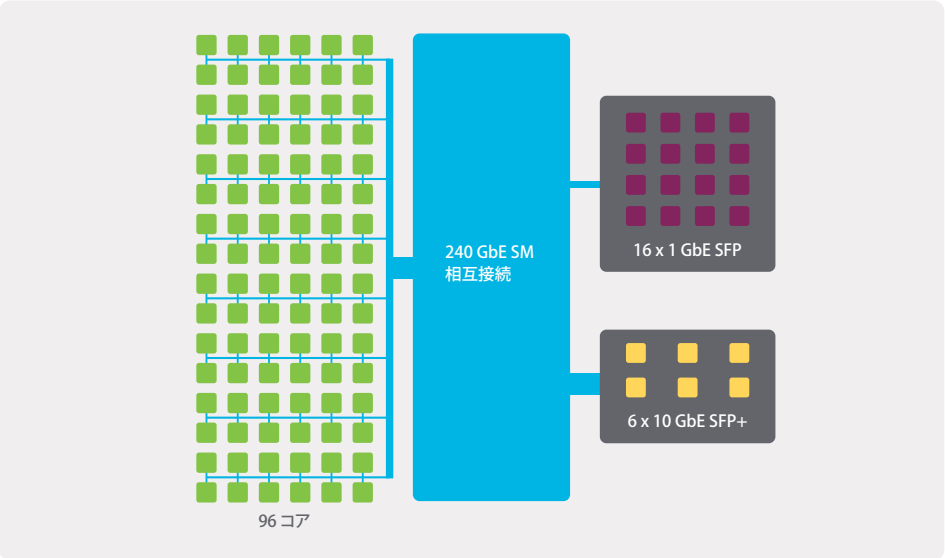
SSL 復号化などの必要な前処理を施したパケットは、侵入攻撃、マルウェア、アプリケーションの 3 つのシグネチャデータベースをまとめた単一の独自メモリに照らして分析されます。これにより、接続の状態は各データベースに応じたストリームの位置まで進められ、それが攻撃やその他の「一致」イベントの状態に至ると、事前に設定されたアクションが実行されます。ほとんどの場合は接続が中断され、適切なログと通知イベントが作成されます。エンジンを検出専用に設定することもできます。また、アプリケーション検出の場合は、アプリケーションが識別されたら、ただちに残りのアプリケーションストリームにレイヤ 7 の帯域幅管理サービスを提供することもできます。



優れた拡張性とパフォーマンスを実現する拡張可能なアーキテクチャ

RFDPI エンジンは、高いパフォーマンスでセキュリティスキャンを実行することに主眼を置いてーから設計されており、本質的に並列で増加し続けるというネットワークトラフィックの性質に沿っています。この並列処理重視のソフトウェアアーキテクチャと 24、32、48、64、または 96 コアのプロセッサーシステムの組み合わせは、高負荷トラフィックでのディープ・パケット・インスペクション（DPI）の要求にも応えることができる完全な拡張性を有しています。SuperMassive プラットフォームでは、x86 プロセッサーとは異なる、パケット、暗号、ネットワークの処理に最適化されたプロセッサーが使用されており、ASIC システムの弱点である現場での柔軟性とプログラム性が確保されています。こうした柔軟性は、最新の高度な検出技術を必要とする新たな攻撃を防ぐために、新しいコードや動作を更新しなければならない状況では不可欠なものです。

このプラットフォーム設計のもうひとつの特徴として、システムの任意のコアで新しい接続を確立するための独自機能が備わっていることが挙げられます。これにより、非常に優れた拡張性が実現し、トラフィックの急増にも対処できます。このアプローチにより、ディープ・パケット・インスペクションを実行しながらも、新規セッションの確立レート（新規接続数/秒）を非常に高くすることができます。これは、データセンターへの導入でボトルネックになることが多い重要な指標です。



SONICWALL™

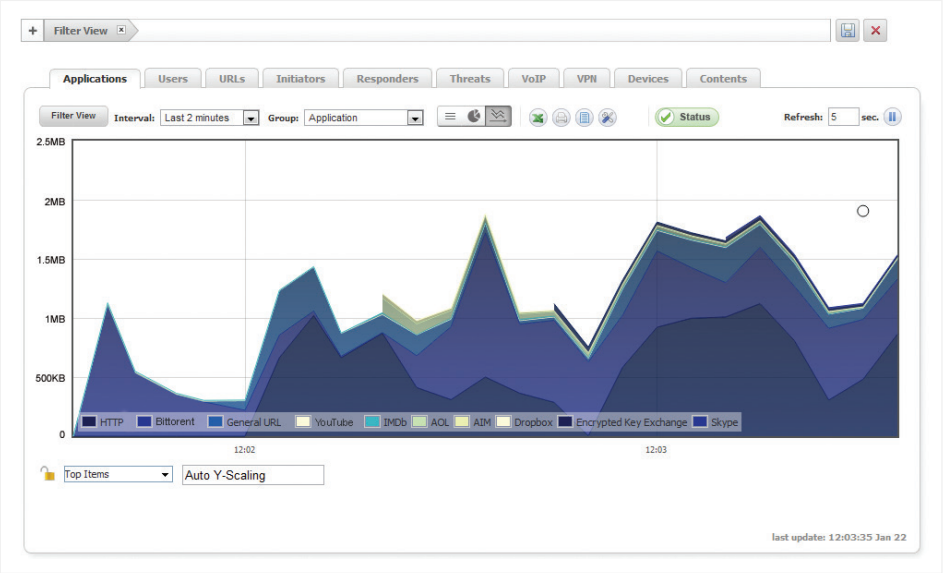
セキュリティと保護

SonicWall の社内に設置された専任の脅威調査チームは、実際のファイアウォールに導入して最新の保護を実現するための対抗策の研究と開発に取り組んでいます。このチームは、世界中の 100 万個を超えるセンサーを活用してマルウェアのサンプルを収集し、最新の脅威情報に関するテレメトリフィードバックを得ています。その成果は、侵入防止、アンチマルウェア、アプリケーション検出の機能に活かされています。最新のセキュリティ機能を備えた SonicWall NGFW のお客様は、24 時間体制で継続的に更新される脅威防御を享受できます。更新内容は再起動や中断を伴わずに即座に適用されます。アプライアンスに搭載されているシグネチャは幅広い攻撃を防御し、1 つのシグネチャで何万もの異なる脅威に対応します。

SuperMassive ファイアウォールでは、付属の対抗策に加えて SonicWall CloudAV サービスを利用することもできます。これにより、標準装備のシグネチャインテリジェンスが拡張され、1,700 万以上のシグネチャを利用できるようになります（この数は増え続けています）。ファイアウォールは専用の軽量プロトコルを介して CloudAV データベースにアクセスし、実行する検査を補強します。また、クラウドベースのネットワークサンドボックスである Capture Advanced Threat Protection により、組織は隔離された環境で疑わしいファイルやコードを検査して、ゼロデイ攻撃などの高度な脅威を阻止することができます。

アプリケーションインテリジェンスおよびコントロール

アプリケーションインテリジェンスを通じて、管理者はネットワークを横断するアプリケーショントラフィックに関する情報を入手します。その情報に基づいて、業務の優先度に応じたアプリケーションコントロールをスケジュールし、非生産的なアプリケーションのトラフィックを制限したり、潜在的に危険なアプリケーションをブロックできます。リアルタイムの可視化により、発生したトラフィックの異常をただちに識別し、想定されるインバウンド/アウトバウンド攻撃やパフォーマンスのボトルネックに対して即座に対抗策をとることができます。



SonicWall のアプリケーショントラフィック分析機能を使用すると、アプリケーショントラフィック、帯域幅の使用状況、セキュリティの脅威について詳しく知ることができます。加えて、トラブルシューティングやフォレンジックのための強力な機能も利用できます。さらに、安全なシングルサインオン（SSO）機能により、ユーザーエクスペリエンスと生産性が向上し、サポートコールの回数が減少します。直感的な Web ベースのインターフェイスが、アプリケーションインテリジェンスおよびコントロールの管理を簡素化します。

グローバルな管理とレポート機能

大規模な分散エンタープライズ環境への導入では、オプションの SonicWall Global Management System（GMS®）を使用することで、統合された安全で包括的なプラットフォームで SonicWall のセキュリティアプライアンスを管理できます。GMS により、企業はセキュリティアプライアンスの管理を容易に統合し、管理やトラブルシューティングに伴う複雑さを軽減して、ポリシーの一元管理と適用、リアルタイムでのイベント監視、分析、レポート作成など、セキュリティインフラストラクチャのあらゆる運用を制御できます。さらに、ワークフローの自動化機能により、GMS は企業のファイアウォール変更管理のニーズにも対応します。

GMS のワークフロー自動化を使用することで、すべての企業は、規制に適合した適切なファイアウォールポリシーを、確信をもってタイムリーかつ迅速に導入できます。GMS を使用すると、ビジネスプロセスやサービスレベルに基づいて効率的にネットワークセキュリティを管理できます。デバイスごとの管理と比べると、セキュリティ環境全体のライフサイクル管理が大幅に簡素化されます。

SONICWALL™

機能

RFDPI エンジン	
機能	説明
Reassembly-Free Deep Packet Inspection（RFDPI）	この特許取得済みの当社独自の高性能なインスペクションエンジンは、プロキシやバッファリングなしでストリームベースの双方向トラフィック分析を実行し、侵入の試みやマルウェアを発見して、すべてのポートでアプリケーショントラフィックを識別します。
双方向インスペクション	インバウンドトラフィックとアウトバウンドトラフィックの両方で同時に脅威をスキャンすることで、ネットワークがマルウェアの配布に使用されるのを防ぎ、感染したマシンが持ち込まれた場合にネットワークが攻撃のプラットフォームになるのを防ぎます。
ストリームベースのインスペクション	プロキシやバッファリングが不要なインスペクション技術により、何百万もの同時ネットワークストリームの DPI を、ファイルやストリームのサイズ制限を設けずに、きわめて小さなレイテンシで実行します。さらに、一般的なプロトコルだけでなく TCP の生ストリームにもこの技術を適用できます。
高度な並列性および拡張性	独自設計の RFDPI エンジンがマルチコアアーキテクチャと連携することで優れた DPI スループットが実現し、新規セッション確立速度も非常に高くなり、要求の厳しいネットワークのトラフィック急増にも対処できます。
シングルパスインスペクション	シングルパス DPI アーキテクチャでは、マルウェア、侵入、アプリケーション特定が同時にスキャンされるため、DPI のレイテンシが大幅に減少し、単一のアーキテクチャの中ですべての脅威情報が関連付けられます。

Capture Advanced Threat Protection	
機能	説明
マルチエンジンのサンドボックス	仮想サンドボックス、フル・システム・エミュレーション、ハイパーバイザレベルの分析技術を備えたマルチエンジンのサンドボックスプラットフォームが、疑わしいコードを実行して動作を分析します。これにより、悪意のあるアクティビティが全面的に可視化されます。
さまざまな種類とサイズのファイル分析	実行可能プログラム（PE）、DLL、PDF、MS Office ドキュメント、アーカイブ、JAR、APK など、さまざまな種類のファイルを分析します。さらに、複数のオペレーティングシステム（Windows、Android、Mac OS X）やマルチブラウザ環境にも対応します。
シグネチャの迅速な導入	悪意のあるファイルが特定されると、SonicWall Capture サブスクリプションが有効なファイアウォールに対してシグネチャがただちに配布されます。また、GRID ゲートウェイアンチウイルスおよび IPS シグネチャのデータベース、加えて URL、IP、ドメインレピュテーションのデータベースにも脅威の情報が 48 時間以内に送られます。
判定が下るまでブロック	悪意がある可能性のあるファイルがネットワークに侵入するのを防ぐため、分析のためにクラウドへ送信したファイルを判定が下るまでゲートウェイで保持できます。

侵入防止	
機能	説明
対抗策ベースの保護	緊密に統合された侵入防止システム（IPS）では、シグネチャその他の対抗策を活用してパケットペイロードに脆弱性やエクスプロイトがないかスキャンし、攻撃や脆弱性に幅広く対処します。
シグネチャの自動更新	SonicWall の脅威調査チームは継続的に脅威を研究し、50 以上の攻撃分野をカバーする IPS 対抗策の広範なリストを随時更新しています。更新内容は再起動やサービスの中断を伴わずに即座に適用されます。
ゾーン内での IPS 保護	侵入防止機能を備えた複数のセキュリティゾーンにネットワークをセグメント化し、脅威がゾーンの境界を越えて拡大するのを阻止することで内部セキュリティを強化します。
ボットネットによるコマンドとコントロール（CnC）の検出とブロック	ローカルネットワーク上のボットが、マルウェアの拡散元として特定された IP やドメイン、または既知の CnC ポイントである IP やドメインに向けて CnC トラフィックを送信した場合に、それを特定してブロックします。
プロトコルの不正使用/異常の検出と防止	プロトコルを悪用して IPS をひそかに通過しようとする攻撃を特定してブロックします。
ゼロデイ防御	何千種類にもおよぶエクスプロイトの最新の方法や技術に対抗できるように随時更新することで、ゼロデイ攻撃からネットワークを保護します。
回避防止テクノロジー	ストリームの大規模な正規化、デコード、およびその他の技術により、レイヤ 2〜7 の検出回避手法を用いた脅威がネットワークに侵入するのを防ぎます。

脅威防御	
機能	説明
ゲートウェイアンチマルウェア	RFDPI エンジンは、インバウンドトラフィック、アウトバウンドトラフィック、ゾーン内のトラフィックをすべてスキャンして、ウイルス、トロイの木馬、キーロガー、その他のマルウェアがファイルにないか調べます。すべてのポートと TCP ストリームのファイルが対象となり、長さやサイズに制限はありません。
CloudAV	SonicWall のクラウドサーバーには 1700 万件を超える脅威のシグネチャを格納したデータベースがあり、その内容は継続的に更新されています。このデータベースを参照することで、機器上のシグネチャデータベースの機能を補強し、RFDPI で扱う脅威の範囲を拡大できます。
24 時間体制のセキュリティ更新	SonicWall の脅威調査チームは、24 時間、週 7 日体制で新たな脅威を分析し、対抗策を生み出しています。新たな脅威の更新は、セキュリティサービスが有効な現地のファイアウォールへ自動的に送信され、再起動や中断を伴わずに即座に適用されます。
SSL インスペクション	SSL トラフィックを復号化し、マルウェア、侵入、データ漏洩がないかプロキシ化せずにその場で検査します。さらに、アプリケーション、URL、コンテンツのコントロールポリシーを適用して、SSL で暗号化されたトラフィックに潜む脅威を防御します。
双方向の生の TCP インスペクション	RFDPI エンジンはすべてのポートで TCP の生ストリームを双方向でスキャンできるため、少数のウェルノウンポートだけを保護する旧式のセキュリティシステムをすり抜けようとする攻撃でも阻止できます。
広範なプロトコルのサポート	HTTP/S、FTP、SMTP、SMBv1/v2 など、生の TCP でデータを送信しない一般的なプロトコルを識別し、標準のウェルノウンポートで実行されていない場合でもペイロードをデコードしてマルウェアを検査します。

機能

アプリケーションインテリジェンスおよびコントロール	
機能	説明
アプリケーションコントロール	RFDPI エンジンは、3,600 以上のアプリケーションシグネチャを格納した、拡張し続けるデータベースに照らして識別されたアプリケーションやその諸機能を制御し、ネットワークのセキュリティと生産性を高めます。
カスタムアプリケーションの識別	特定のパラメータまたはアプリケーション固有のネットワーク通信パターンに基づいてシグネチャを作成することで、カスタムアプリケーションを制御し、ネットワークの管理を強化します。
アプリケーションの帯域幅管理	重要なアプリケーションまたは重要なアプリケーションカテゴリに対しては帯域幅の割り当てと調整をきめ細かく行い、重要性の低いアプリケーションのトラフィックは抑制します。
オンボックス/オフボックスのトラフィック可視化	オンボックスのアプリケーショントラフィックのリアルタイム可視化と、NetFlow/IPFix を介したオフボックスのアプリケーショントラフィックのレポート機能により、帯域幅使用率を識別してネットワークの動作を分析します。
詳細なコントロール	LDAP/AD/Terminal Services/Citrix 統合による SSO ユーザーの完全な識別により、スケジュール、ユーザーグループ、除外リスト、各種アクションに基づいてアプリケーションやその特定コンポーネントを制御します。

コンテンツフィルタリング	
機能	説明
内部/外部のコンテンツフィルタリング	コンテンツ・フィルタリング・サービスは、使用ポリシーを適用することによって、好ましくない、または非生産的な情報や画像を掲載している Web サイトへのアクセスをブロックします。コンテンツ・フィルタリング・クライアントは、ポリシーの適用範囲を拡大し、ファイアウォールの境界外にあるデバイスに対してもインターネットコンテンツをブロックします。
詳細なコントロール	事前定義されているカテゴリまたはカテゴリの組み合わせを使用してコンテンツをブロックします。授業時間や営業時間などの時間帯でフィルタリングをスケジュールし、個々のユーザーやグループに適用できます。
動的なレーティングアーキテクチャ	要求されたすべての Web サイトは、動的に更新されるクラウドのデータベースで相互参照されます。このデータベースは、数百万件の URL、IP アドレス、ドメインをリアルタイムで分類します。
学校向け YouTube	教師は YouTube EDU にアップロードされている無数の教育用無料動画の中から選択できます。YouTube EDU は科目/学年別に編成されており、共通の教育基準に沿っています。
Web キャッシュ	URL のレーティングは SonicWall ファイアウォールでローカルにキャッシュされるため、頻繁に訪問するサイトの場合、以降のアクセスに要する応答時間はほんの一瞬です。

アンチウイルス/アンチスパイウェアの適用	
機能	説明
マルチレイヤ保護	ファイアウォールのゲートウェイ・アンチウイルス・ソリューションは、境界を保護する最初のレイヤとなります。しかし、ノートパソコンや USB メモリ、その他の保護されていないシステムを介してウイルスはネットワークに侵入することができます。多層的なアプローチを採用することで、アンチウイルス/アンチスパイウェア対策をクライアントとサーバーの両方に広げることができます。
自動適用	ネットワークにアクセスするコンピューターのすべてに最新バージョンのアンチウイルス/アンチスパイウェアのシグネチャをインストールして有効化します。これにより、デスクトップのアンチウイルス/アンチスパイウェア管理に伴うコストを削減できます。
自動化された導入とインストール	アンチウイルス/アンチスパイウェアクライアントの導入とインストールがネットワーク経由でマシンごとに自動的に行われるため、管理の余分な手間を最小限に抑えることができます。
常に有効な自動ウイルス対策	すべてのデスクトップとファイルサーバーに対してアンチウイルス/アンチスパイウェアの更新が頻繁かつ透過的に配信されるため、エンドユーザーの生産性が向上し、セキュリティ管理が軽減されます。
スパイウェア対策	強力なスパイウェア対策により、広範なスパイウェアプログラムをスキャンして、デスクトップやノートパソコンへのインストールをブロックします。これにより、機密データの送信が事前に防止され、デスクトップのセキュリティとパフォーマンスが向上します。

ファイアウォールとネットワーキング	
機能	説明
ステートフル・パケット・インスペクション	すべてのネットワークトラフィックを検査、分析して、ファイアウォールのアクセスポリシーに準拠させます。
DDoS/DoS 攻撃の防御	SYN フラッド防御は、レイヤ 3 SYN プロキシとレイヤ 2 SYN ブラックリストテクノロジーの両方を使用して DOS 攻撃を防御します。さらに、UDP/ICMP フラッド防御と接続率制限によって DOS/DDoS 攻撃を防御することもできます。
柔軟な導入オプション	SuperMassive シリーズは、従来型の NAT、レイヤ 2 ブリッジ、ワイヤモード、ネットワーク・タップ・モードで導入できます。
IPv6 のサポート	インターネット・プロトコル・バージョン 6（IPv6）は、IPv4 から移行する初期段階にあります。最新の SonicOS 6.2 では、ハードウェアでフィルタリングとワイヤモード実装をサポートします。
高可用性/クラスタリング	SuperMassive シリーズは、ステート同期によるアクティブ/パッシブ（A/P）、アクティブ/アクティブ（A/A）DPI、アクティブ/アクティブのクラスタリング高可用性モードをサポートします。アクティブ/アクティブ DPI では、ディープ・パケット・インスペクションの負荷をパッシブアプライアンスのコアにオフロードすることでスループットを引き上げます。
WAN ロードバランシング	ラウンドロビン、スピルオーバー、またはパーセンテージの手法により、複数の WAN インターフェイス間でロードバランシングを行います。
ポリシーベースのルーティング	プロトコルに応じて優先 WAN 接続にトラフィックを転送する経路を作成します。障害が起きた場合は、セカンダリ WAN にフェイルバックする機能を有しています。
高度なサービス品質（QoS）	802.1p、DSCP のタグ付け、ネットワーク上の VoIP トラフィックの再マッピングにより、重要な通信を保証します。
H.323 ゲートキーパーおよび SIP プロキシサポート	H.323 ゲートキーパーまたは SIP プロキシによる認証/承認をすべての受信コールに要求することで、スパムコールをブロックします。

機能

管理およびレポート機能	
機能	説明
Global Management System	SonicWall GMS は、直感的なインターフェイスを備えた単一の管理コンソールで複数の SonicWall アプライアンスを監視、構成、レポートできるため、管理のコストと複雑さを削減できます。
強力な単一デバイスによる管理	直感的な Web ベースのインターフェイスにより、迅速かつ容易な構成が可能です。さらに、包括的なコマンド・ライン・インターフェイスを搭載し、SNMPv2/3 をサポートしています。
IPFIX/NetFlow によるアプリケーションフローのレポート	IPFIX または NetFlow プロトコルを介してアプリケーショントラフィックの分析データと使用状況データをエクスポートし、SonicWall Scrutinizer や、IPFIX/NetFlow を拡張機能でサポートしているその他のツールを使用してリアルタイム/履歴監視やレポート作成を行うことができます。

仮想プライベートネットワーク（VPN）	
機能	説明
サイト間接続のための IPSec VPN	ハイパフォーマンスな IPSec VPN により、SuperMassive シリーズは何千もの他の大規模なサイト、支店、ホームオフィスを接続する VPN コンセントレータの役割を果たします。
SSL VPN または IPSec クライアントのリモートアクセス	クライアントレス SSL VPN テクノロジーまたは管理が容易な IPSec クライアントを使用して、さまざまなプラットフォームから電子メール、ファイル、コンピューター、イントラネットサイト、アプリケーションに簡単にアクセスできます。
冗長 VPN ゲートウェイ	複数の WAN を使用している場合は、プライマリ/セカンダリ VPN を構成して、すべての VPN セッションのフェイルオーバとフェイルバックをシームレスかつ自動的に行うことができます。
ルートベース VPN	VPN リンク経由で動的ルーティングを実行できるため、VPN トンネルに一時的に障害が発生しても、エンドポイント間の代替ルートでトラフィックをシームレスに再ルーティングすることにより、継続的な稼働を維持できます。

コンテンツ/コンテキスト認識	
機能	説明
ユーザーアクティビティの追跡	ユーザーの識別とアクティビティの追跡は、シームレスな AD/LDAP/Citrix/Terminal Services[1] SSO 統合と DPI で取得した広範な情報を併用することで可能になります。
GeoIP による国別のトラフィック識別	特定の国へのトラフィック、または特定の国からのトラフィックを識別して制御し、既知の脅威または疑わしい脅威の発信元からの攻撃を防御したり、ネットワークから発信されている疑わしいトラフィックを調査したりします。
正規表現による DPI フィルタリング	正規表現マッチングにより、ネットワークを通過するコンテンツを識別、制御してデータの漏洩を防ぎます。

[1] *SonicOS 6.1 および 6.2 でサポートされています。SonicOS 6.2.1 ではサポートされていません。*
[2] *サブスクリプションを追加する必要があります。*

SONICWALL™

機能の要約

ファイアウォール

- Reassembly-Free Deep Packet Inspection
- SSL 復号化およびインスペクション
- ステートフル・パケット・インスペクション
- ステルスモード
- Common Access Card（CAC）のサポート
- DoS 攻撃防御
- UDP/ICMP/SYN フラッド防御
- IPv6 セキュリティ
- 管理と監視: IPv4 と IPv6 の管理
- ネットワーク: IPv6

Capture Advanced Threat Protection

- クラウドベースのマルチエンジン分析
- 仮想サンドボックス
- ハイパーバイザレベルの分析
- フル・システム・エミュレーション
- さまざまな種類のファイル調査
- 自動/手動送信
- リアルタイムの脅威インテリジェンス更新
- 自動ブロック機能

侵入防止

- シグネチャベースのスキャン
- シグネチャの自動更新
- 双方向インスペクションエンジン
- 詳細な IPS ルールセット
- GeoIP および評価ベースのフィルタリング
- 正規表現マッチング
- UDP/ICMP/SYN フラッド防御

アンチマルウェア

- ストリームベースのマルウェアスキャン
- ゲートウェイアンチウイルス
- ゲートウェイアンチスパイウェア
- 双方向インスペクション
- ファイルサイズの制限なし
- クラウドのマルウェアデータベース

アプリケーションインテリジェンス

- アプリケーションコントロール
- アプリケーションコンポーネントのブロック
- アプリケーションの帯域幅管理
- カスタムアプリケーションのシグネチャ作成
- アプリケーショントラフィックの可視化
- データ漏洩防止
- NetFlow/IPFIX によるアプリケーション レポート機能
- ユーザーアクティビティの追跡（SSO）
- 包括的なアプリケーションシグネチャの データベース

Web コンテンツフィルタリング

- URL フィルタリング
- アンチプロキシテクノロジー
- キーワードブロック
- CFS カテゴリの帯域幅管理
- アプリケーションコントロール可能な統合 ポリシーモデル
- 56 のコンテンツ・フィルタリング・カテゴリ
- コンテンツ・フィルタリング・クライアント （SonicOS 6.2）

VPN

- サイト間接続のための IPSec VPN
- SSL VPN および IPSec クライアントの リモートアクセス
- 冗長 VPN ゲートウェイ
- Apple® iOS と Google® Android™ の モバイル接続
- ルートベース VPN（OSPF、RIP）

ネットワーク

- ジャンボフレーム（SonicOS 6.0.5 および 6.2 のみ）
- パス MTU 検出
- 強化されたログ機能
- VLAN トランキング
- レイヤ 2 ネットワーク検出
- ポートミラーリング
- レイヤ 2 QoS
- ポートセキュリティ
- 動的ルーティング
- SonicPoint ワイヤレスコントローラ
- ポリシーベースのルーティング
- 先進的な NAT
- DHCP サーバー
- 帯域幅管理
- リンクアグリゲーション
- ポートの冗長性
- ステートシンクによる A/P 高可用性
- A/A クラスタリング
- インバウンド/アウトバウンドのロード バランシング
- L2 ブリッジ、ワイヤモード、タップモード、 NAT モード

VoIP

- 詳細な QoS コントロール
- 帯域幅管理
- VoIP トラフィックに対する DPI
- H.323 ゲートキーパーおよび SIP プロキシ サポート

管理と監視

- Web GUI
- コマンド・ライン・インターフェイス（CLI）
- SNMPv2/v3
- すぐに使えるレポート機能（Scrutinizer）
- SonicWall Global Management System （GMS）による一元的な管理とレポート 機能
- ログ
- Netflow/IPFix エクスポート
- アプリケーションと帯域幅の可視化
- LCD 管理画面
- シングルサインオン（SSO）
- ターミナルサービス/Citrix サポート
- BlueCoat Security Analytics Platform

SuperMassive E10000 シリーズのシステム仕様

	E10400	E10800
オペレーティングシステム	SonicOS	
セキュリティ・プロセッシング・コア	48	96
10 GbE インターフェイス	6 x 10 GbE SFP+	
1 GbE インターフェイス	16 x 1 GbE SFP	
管理インターフェイス	1 GbE、1 コンソール	
メモリ(RAM)	32 GB	64 GB
ストレージ	80 GB SSD、フラッシュ	
ファイアウォールインスペクションのスループット[1]	20 Gbps	40 Gbps
アプリケーションインスペクションのスループット[2]	15 Gbps	30 Gbps
IPS のスループット[2]	15 Gbps	28 Gbps
アンチマルウェアインスペクションのスループット[2]	6 Gbps	12 Gbps
IMIX のパフォーマンス	4.3 Gbps	9 Gbps
SSL-DPI のパフォーマンス	3 Gbps	5 Gbps
VPN のスループット[3]	7.5 Gbps	11 Gbps
レイテンシ	24 µs	
接続数/秒	200,000/秒	400,000/秒
最大接続数(SPI)	6 M	12 M
最大接続数(DPI)	5 M	10 M
SSO ユーザー数	40,000	60,000
VPN	**E10400**	**E10800**
サイト間トンネル数	10,000	
IPSec VPN クライアント数(最大)	2,000(10,000)	
暗号化	DES、3DES、AES(128、192、256 ビット)	
認証	MD5、SHA-1、Common Access Card (CAC)	
キー交換	Diffie Hellman グループ 1、2、5、14	
ルートベース VPN	RIP、OSPF	
ネットワーク	**E10400**	**E10800**
IP アドレス割り当て	静的、内部 DHCP サーバー、DHCP リレー	
NAT モード	1 対 1、多対 1、1 対多、フレキシブル NAT(重複 IP)、PAT、トランスペアレントモード	
VLAN インターフェイス	1024	2048
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースルーティング、マルチキャスト	
QoS	帯域幅の優先度、最大帯域幅、保証帯域幅、DSCP マーキング、802.1p	
認証	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザーデータベース、ターミナルサービス、Citrix	
VoIP	フル H323-v1-5、SIP	
標準	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3	
認定	FIPS 140-2、コモンクライテリア NDPP、IPv6 Phase 2、VPAT、VPNC	
第三者機関による検証	NSS の NGFW 部門で「Recommended (推奨)」、NSS の IPS 部門で「Recommended (推奨)」	
ハードウェア	**E10400**	**E10800**
電源	デュアル冗長、ホットスワップ可能、850 W	
ファン	デュアル冗長、ホットスワップ可能	
ディスプレイ	前面 LED ディスプレイ	
電源入力	100〜240 VAC、50〜60 Hz	
最大消費電力(W)	550	750
MTBF (25 °C、単位は時間)	120,790	
MTBF (25 °C、単位は年)	13.789	
フォームファクタ	4U ラックマウント型	
寸法	43 x 43.5 x 17.8 cm (17 x 18 x 7 インチ)	
重量	27.7 kg (61 ポンド)	30.3 kg (67 ポンド)
WEEE 重量	28.1 kg (62 ポンド)	30.8 kg (68 ポンド)
出荷時の重量	37.2 kg (82 ポンド)	39.9 kg (88 ポンド)
主な規制	FCC Class A、CE、C-Tick、VCCI、Compliance MIC、UL、cUL、TUV/GS、CB、NOM、RoHS、WEEE	
環境	5〜40 °C、40〜105 °F	
湿度	10〜90% (結露しないこと)	

[1] テスト手法: 最大パフォーマンスは RFC 2544 (ファイアウォール) に基づいています。実際のパフォーマンスは、ネットワークの状態と使用するサービスによって異なる場合があります。[2] フル DPI/ゲートウェイアンチウイルス/アンチスパイウェア/IPS のスループットは、業界標準の Spirent WebAvalanche HTTP パフォーマンス・テスト・ツールと Ixia テストツールを使用して測定しています。テストには、複数のポートペアで複数のフローを使用しました。[3] VPN のスループットは、RFC 2544 準拠のパケットサイズ 1,280 バイトの UDP トラフィックを使用して測定しています。すべての仕様、機能、入手可能性は変更されることがあります。

SONICWALL™

SuperMassive 9000 シリーズのシステム仕様

	9200	9400	9600	9800
オペレーティングシステム	SonicOS			
セキュリティ・プロセッシング・コア	24	32		64
10 GbE インターフェイス	4 x 10 GbE SFP+			
1 GbE インターフェイス	8 x 1 GbE SFP、8 x 1 GbE（1 LAN バイパスペア）			12 x 1 GbE SFP、8 x 1 GbE
管理インターフェイス	1 GbE、1 コンソール			
メモリ（RAM）	8 GB	16 GB	32 GB	64 GB
ストレージ	フラッシュ			2 x 80 GB SSD、フラッシュ
拡張	1 拡張スロット（背面）*、SD カード*			
ファイアウォールインスペクションのスループット[1]	15 Gbps	20 Gbps		40 Gbps
アプリケーションインスペクションのスループット[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
IPS のスループット[2]	5 Gbps	10 Gbps	11.5 Gbps	24 Gbps
アンチマルウェアインスペクションのスループット[2]	3.5 Gbps	4.5 Gbps	5 Gbps	10 Gbps
IMIX のパフォーマンス	4.4 Gbps	5.5 Gbps		9 Gbps
SSL-DPI	1 Gbps	2 Gbps	2 Gbps	5 Gbps
VPN のスループット[3]	5 Gbps	10 Gbps	11.5 Gbps	18 Gbps
レイテンシ	17 µs			
接続数/秒	100,000/秒	130,000/秒		280,000/秒
最大接続数（SPI）	1.25 M		1.5 M	3 M
最大接続数（DPI）	1 M		1.25 M	2.5 M
SSO ユーザー数	80,000	90,000	100,000	110,000
サポートされる SonicPoint の最大数	128			-
VPN	**9200**	**9400**	**9600**	**9800**
サイト間トンネル数	10,000			25,000
IPSec VPN クライアント数（最大）	2,000（4,000）	2,000（6,000）	2,000（10,000）	2,000（10,000）
暗号化/認証	DES、3DES、AES（128、192、256 ビット）/MD5、SHA-1、Suite B、Common Access Card（CAC）			
キー交換	Diffie Hellman グループ 1、2、5、14v			
ルートベース VPN	RIP、OSPF			
ネットワーク	**9200**	**9400**	**9600**	**9800**
IP アドレス割り当て	静的、DHCP、PPPoE、L2TP および PPTP クライアント、内部 DHCP サーバー、DHCP リレー[4]			
NAT モード	1 対 1、多対 1、1 対多、フレキシブル NAT（重複 IP）、PAT、トランスペアレントモード			
VLAN インターフェイス	512			
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースルーティング、マルチキャスト			
QoS	帯域幅の優先度、最大帯域幅、保証帯域幅、DSCP マーキング、802.1p			
認証	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザーデータベース、ターミナルサービス[5]、Citrix[5]			
VoIP	フル H323-v1-5、SIP			
標準	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3			
認定	UC APL[4]、ICSA エンタープライズファイアウォール、IPV6 Phase 2、VPNC、VPAT、FIPS 140-2[4]、コモンクライテリア NDPP[4]			
認定審査中	ICSA アンチウイルス			
ハードウェア	**9200**	**9400**	**9600**	**9800**
電源	デュアル冗長、ホットスワップ可能、300 W			デュアル冗長、ホットスワップ可能、500 W
ファン	デュアル冗長、ホットスワップ可能			
ディスプレイ	前面 LED ディスプレイ			
電源入力	100～240 VAC、50～60 Hz			
最大消費電力（W）	200			350
MTBF（25 °C、単位は時間）	188,719	187,702	186,451	126,144
MTBF（25 °C、単位は年）	21.543	21.427	21.284	14.400
フォームファクタ	1U ラックマウント型			2U ラックマウント型
寸法	43.3 x 48.5 x 4.5 cm（17 x 19.1 x 1.75 インチ）			43 x 60 x 9 cm（17 x 24 x 3.5 インチ）
重量	8.2 kg（18.1 ポンド）			18.38 kg（40.5 ポンド）
WEEE 重量	10.4 kg（23 ポンド）			22.4 kg（49.5 ポンド）
出荷時の重量	13.3 kg（29.3 ポンド）			29.64 kg（65 ポンド）
主な規制	FCC Class A、CE、C-Tick、VCCI、Compliance KCC、UL、cUL、TUV/GS、CB、NOM、RoHS、WEEE、ANATEL、BSMI			
環境	0～40 °C、32～105 °F			15～40 °C
湿度	10～90%（結露しないこと）			

*[1] テスト手法: 最大パフォーマンスは RFC 2544（ファイアウォール）に基づいています。実際のパフォーマンスは、ネットワークの状態と使用するサービスによって異なる場合があります。[2] フル DPI/ゲートウェイアンチウイルス/アンチスパイウェア/IPS のスループットは、業界標準の Spirent WebAvalanche HTTP パフォーマンス・テスト・ツールと Ixia テストツールを使用して測定しています。テストには、複数のポートペアで複数のフローを使用しました。[3] VPN のスループットは、RFC 2544 準拠のパケットサイズ 1,280 バイトの UDP トラフィックを使用して測定しています。[4] SM9800 では PPPoE、L2TP および PPTP クライアントはサポートされていません。[5] SonicOS 6.1 および 6.2 でサポートされています。[4] SuperMassive 9200、9400、9600 に適用されます。SuperMassive 9800 UC APL の認定は審査中です。*将来用。すべての仕様、機能、入手可能性は変更されることがあります。*

SuperMassive E10000 シリーズの注文情報

製品	SKU
SuperMassive E10400、SFP+ 10 GbE ポート x 6、SFP 1 GbE ポート x 16、デュアルファン、デュアル AC 電源	01-SSC-8881
SuperMassive E10800、SFP+ 10 GbE ポート x 6、SFP 1 GbE ポート x 16、デュアルファン、デュアル AC 電源	01-SSC-8856
システムのアップグレード	**SKU**
SuperMassive E10200 から E10400 へのアップグレード	01-SSC-9497
SuperMassive E10400 から E10800 へのアップグレード	01-SSC-9498
SuperMassive E10400 のサポートおよびセキュリティサブスクリプション	**SKU**
脅威防御: E10400 用の侵入防止、ゲートウェイアンチウイルス、ゲートウェイアンチスパイウェア、クラウドアンチウイルス（1 年間）	01-SSC-9536
アプリケーションインテリジェンスおよびコントロール: E10400 用のアプリケーションインテリジェンス、アプリケーションコントロール、アプリケーションフロー可視化（1 年間）	01-SSC-9542
E10400 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-9539
SuperMassive E10400 用のプレミアムサポート（1 年間）	01-SSC-9548
Comprehensive Gateway Security Suite: E10400 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-9551
SuperMassive E10800 のサポートおよびセキュリティサブスクリプション	**SKU**
アプリケーションインテリジェンスおよびコントロール: E10800 用のアプリケーションインテリジェンス、アプリケーションコントロール、アプリケーションフロー可視化（1 年間）	01-SSC-9560
脅威防御: E10800 用の侵入防止、ゲートウェイアンチウイルス、ゲートウェイアンチスパイウェア、クラウドアンチウイルス（1 年間）	01-SSC-9554
E10800 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-9557
SuperMassive E10800 用のプレミアムサポート（1 年間）	01-SSC-9566
Comprehensive Gateway Security Suite: E10800 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-9569
モジュールおよびアクセサリ*	**SKU**
SuperMassive E10000 シリーズのシステムファン FRU（現場交換可能ユニット）	01-SSC-8885
SuperMassive E10000 シリーズの SSD ファンモジュール	01-SSC-8886
SuperMassive E10000 シリーズの電源 FRU	01-SSC-8887
10G BASE-SR SFP+ 短距離モジュール	01-SSC-9785
10G BASE-LR SFP+ 長距離モジュール	01-SSC-9786
10G BASE SFP+ 1M Twinax ケーブル	01-SSC-9787
10G BASE SFP+ 3M Twinax ケーブル	01-SSC-9788
1000BASE-SX SFP 短距離モジュール	01-SSC-9789
1000BASE-LX SFP 長距離モジュール	01-SSC-9790
1000BASE-T SFP 銅線モジュール	01-SSC-9791
管理およびレポート機能	**SKU**
SonicWall GMS 10 ノードのソフトウェアライセンス	01-SSC-3363
SonicWall GMS E-Class 10 ノードの週 7 日 24 時間ソフトウェアサポート（1 年間）	01-SSC-6514
SonicWall Scrutinizer 仮想アプライアンスおよび最大 5 ノードの Flow Analytics Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-3443
SonicWall Scrutinizer および最大 5 ノードの Flow Analytics Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-4002
SonicWall Scrutinizer および最大 5 ノードの Advanced Reporting Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-3773

*サポートされている SFP および SFP+ モジュールの完全なリストについては、デルの SE にお問い合わせください。

SONICWALL™

SuperMassive 9000 シリーズの注文情報

製品	SKU
SuperMassive 9800	01-SSC-0200
SuperMassive 9800 高可用性	01-SSC-0801
SuperMassive 9600	01-SSC-3880
SuperMassive 9600 高可用性	01-SSC-3881
SuperMassive 9400	01-SSC-3800
SuperMassive 9400 高可用性	01-SSC-3801
SuperMassive 9200	01-SSC-3810
SuperMassive 9200 高可用性	01-SSC-3811
SuperMassive 9200 のサポートおよびセキュリティサブスクリプション	**SKU**
先進的なゲートウェイ・セキュリティ・スイート: SuperMassive 9200 用の Capture ATP、脅威防御、コンテンツフィルタリング、週 7 日 24 時間のサポート（1 年間）	01-SSC-1570
SuperMassive 9200 用の Capture Advanced Threat Protection（1 年間）	01-SSC-1575
Comprehensive Gateway Security Suite: 9200 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-4172
SuperMassive 9200 用の侵入防御、アンチマルウェア、CloudAV、アプリケーションインテリジェンス、コントロールおよび可視化（1 年間）	01-SSC-4202
9200 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-4184
SuperMassive 9200 用のプレミアムサポート（1 年間）	01-SSC-4178
SuperMassive 9400 のサポートおよびセキュリティサブスクリプション	**SKU**
先進的なゲートウェイ・セキュリティ・スイート: SuperMassive 9400 用の Capture ATP、脅威防御、コンテンツフィルタリング、週 7 日 24 時間のサポート（1 年間）	01-SSC-1580
SuperMassive 9400 用の Capture Advanced Threat Protection（1 年間）	01-SSC-1585
Comprehensive Gateway Security Suite: 9400 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-4136
SuperMassive 9400 用の侵入防御、アンチマルウェア、CloudAV、アプリケーションインテリジェンス、コントロールおよび可視化（1 年間）	01-SSC-4166
9400 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-4148
SuperMassive 9400 用のプレミアムサポート（1 年間）	01-SSC-4142
SuperMassive 9600 のサポートおよびセキュリティサブスクリプション	**SKU**
先進的なゲートウェイ・セキュリティ・スイート: SuperMassive 9600 用の Capture ATP、脅威防御、コンテンツフィルタリング、週 7 日 24 時間のサポート（1 年間）	01-SSC-1590
SuperMassive 9600 用の Capture Advanced Threat Protection（1 年間）	01-SSC-1595
Comprehensive Gateway Security Suite: 9600 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-4100
SuperMassive 9600 用の侵入防御、アンチマルウェア、CloudAV、アプリケーションインテリジェンス、コントロールおよび可視化（1 年間）	01-SSC-4130
9600 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-4112
SuperMassive 9600 用のプレミアムサポート（1 年間）	01-SSC-4106
SuperMassive 9800 のサポートおよびセキュリティサブスクリプション	**SKU**
Comprehensive Gateway Security Suite: 9800 用のアプリケーションインテリジェンス、脅威防御、コンテンツフィルタリング、サポート付き（1 年間）	01-SSC-0809
SuperMassive 9800 用の侵入防御、アンチマルウェア、CloudAV、アプリケーションインテリジェンス、コントロールおよび可視化（1 年間）	01-SSC-0827
9800 用のコンテンツフィルタリング Premium Business エディション（1 年間）	01-SSC-0821
SuperMassive 9800 用の週 7 日 24 時間ゴールド サポート（1 年間）	01-SSC-0815
モジュールおよびアクセサリ*	**SKU**
SonicWall SuperMassive 9800 シリーズのシステムファン FRU	01-SSC-0204
SonicWall SuperMassive 9800 シリーズの電源 AC FRU	01-SSC-0203
SonicWall SuperMassive 9000 シリーズのシステムファン FRU	01-SSC-3876
SonicWall SuperMassive 9000 シリーズの電源 AC FRU	01-SSC-3874
10G BASE-SR SFP+ 短距離モジュール	01-SSC-9785
10G BASE-LR SFP+ 長距離モジュール	01-SSC-9786
1000BASE-SX SFP 短距離モジュール	01-SSC-9789
1000BASE-LX SFP 長距離モジュール	01-SSC-9790
1000BASE-T SFP 銅線モジュール	01-SSC-9791
管理およびレポート機能	**SKU**
SonicWall GMS 10 ノードのソフトウェアライセンス	01-SSC-3363
SonicWall GMS E-Class 10 ノードの週 7 日 24 時間ソフトウェアサポート（1 年間）	01-SSC-6514
SonicWall Scrutinizer 仮想アプライアンスおよび最大 5 ノードの Flow Analytics Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-3443
SonicWall Scrutinizer および最大 5 ノードの Flow Analytics Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-4002
SonicWall Scrutinizer および最大 5 ノードの Advanced Reporting Module ソフトウェアライセンス（1 年間の週 7 日 24 時間ソフトウェアサポート付き）	01-SSC-3773

*サポートされている SFP および SFP+ モジュールの完全なリストについては、デルの SE にお問い合わせください。

SONICWALL™

SonicWall Inc. 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-SuperMassive-US-KJ-22292-D1

SONICWALL™