SonicWall TZ シリーズ

卓越したセキュリティと最高のパフォーマンスを衝撃的な低 TCO で実現

SonicWall TZ シリーズは、エンタープライズクラスのネットワーク保護を必要とする組織に理想的な次世代のファイアウォール (NGFW) です。

SonicWall TZ シリーズファイアウォールは、オンボックスでクラウドベースのウイルス対策、スパイウェア対策、アプリケーション制御、侵入防御システム (IPS)、および URL フィルタリングから構成された高度なセキュリティサービスによって広い範囲を保護します。最近の暗号化攻撃に対処するため、新しい SonicWall TZ シリーズには、最新の脅威に対抗する、暗号化 SSL 接続を検査できる処理能力が備えられています。X シリーズスイッチとの統合により、一部の TZ シリーズファイアウォールでこれらの追加のポートのセキュリティを直接管理できます。

SonicWall の Global Response Intelligent Defense（GRID）ネットワークが支える SonicWall TZ シリーズは、継続的に更新することで、サイバー犯罪に対する強固なネットワーク防御を維持します。SonicWall TZ シリーズは、遅延はほぼゼロ、ファイルサイズの制限なしで、すべてのポートとプロトコルのあらゆるパッケージのあらゆるバイトをスキャンできます。

この製品は、ギガビット・イーサネット・ポート、オプションの内蔵 802.11ac ワイヤレス*、IPSec および SSL VPN、統合 3G/4G サポートによるフェイルオーバ、負荷バランシング、およびネットワークセグメンテーションといった各種機能を特徴としています。また、SonicWall TZ シリーズの UTM ファイアウォールは、Apple iOS、Google Android、Amazon Kindle、Windows、MacOS、および Linux の各プラットフォームに対する高速でセキュアなモバイルアクセスを提供します。

SonicWall Global Management System (GMS) では、1 つのシステムから SonicWall TZ シリーズファイアウォールを一元的に展開、管理できます。

分散環境のための総合セキュリティ

教育機関や小売店、リモートサイト、ブランチオフィス、および分散型企業は、使用しているファイアウォールと統合できるソリューションを求めています。SonicWall TZ シリーズファイアウォールは、フラッグシップである SuperMassive 次世代ファイアウォールと同じコードベース、同じ保護を共有しています。これによって、リモートサイトの管理を簡易化し、すべての管理者が同じユーザーインターフェイス (UI) を表示できます。ネットワーク管理者は、GMS を使用することで、SonicWall のリモートファイアウォールを一元的に構成、監視、管理できるようになります。高速で安全なワイヤレス接続を追加したことで、SonicWall TZ シリーズでは、保護できる範囲が拡張され、小売サイトやリモートオフィスをしばしば訪れるお客様やゲストも対象になりました。

メリット：

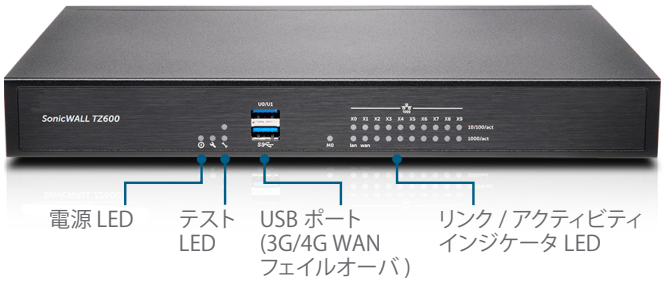
- エンタープライズクラスのネットワーク保護
- ファイルサイズやプロトコルを問わない、あらゆるトラフィックのディープ・パケット・インスペクション
- 内蔵されたワイヤレスコントローラ、または外付の SonicPoint ワイヤレス・アクセス・ポイントを使用したセキュアな 802.11ac ワイヤレス接続
- Apple iOS、Google Android、Amazon Kindle、Windows、Mac OS、および Linux デバイスの SSL VPN モバイルアクセス
- X シリーズスイッチと統合して導入した場合に追加の 100 以上のポートを TZ コンソールで安全に管理可能

** 802.11ac は現在 SOHO モデルでは利用できません。SOHO モデルでは 802.11a/b/g/n をサポートしています。*

SonicWall TZ600 シリーズ

SonicWall TZ600 次世代ファイアウォールは、安価なセキュリティのパフォーマンスを探す新興企業や小売業、ブランチオフィスのための、エンタープライズクラスの各種機能と妥協しないパフォーマンスでネットワークを保護します。

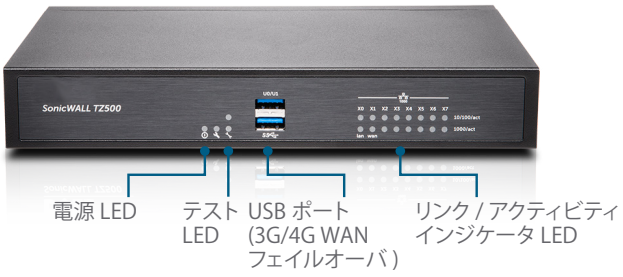
仕様	TZ600 シリーズ
ファイアウォールのスループット	1.5 Gbps
フル DPI のスループット	500 Mbps
マルウェア対策のスループット	500 Mbps
IPS スループット	1.1 Gbps
IMIX スループット	900 Mbps
DPI 最大接続数	125,000
新規接続数 / 秒	12,000

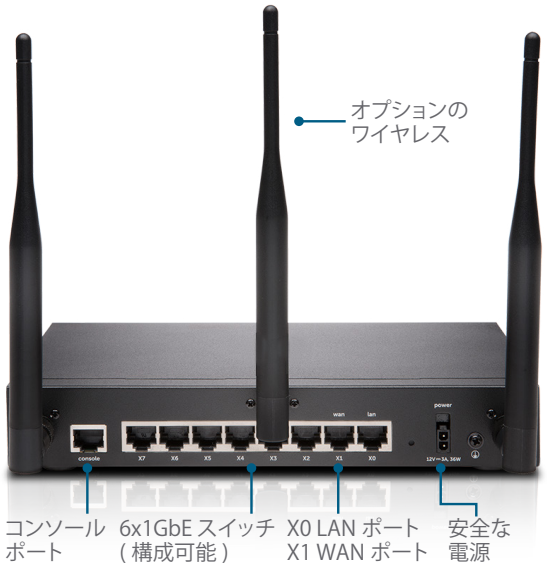


SonicWall TZ500 シリーズ

成長を続けるブランチオフィスや SMB のため、SonicWall TZ500 シリーズは、ネットワークの生産性とオプションの内蔵 802.11ac デュアルバンドワイヤレスにより、きわめて効果的で妥協しない保護を実現します。

仕様	TZ500 シリーズ
ファイアウォールのスループット	1.4 Gbps
フル DPI のスループット	400 Mbps
マルウェア対策のスループット	400 Mbps
IPS スループット	1.0 Gbps
IMIX スループット	700 Mbps
DPI 最大接続数	100,000
新規接続数 / 秒	8,000

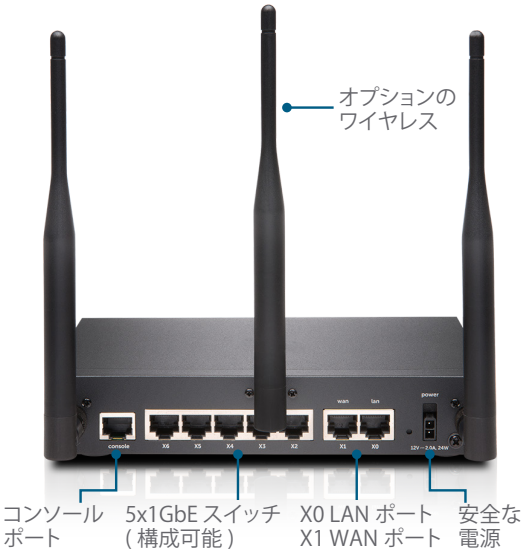




SonicWall TZ400 シリーズ

SonicWall TZ400 シリーズは、スモールビジネス、小売、およびブランチオフィスのための、エンタープライズクラスの保護を提供します。外付の SonicPoint アクセスポイントまたはユニットに内蔵された 802.11ac ワイヤレスいずれかによる、柔軟なワイヤレス環境を展開できます。

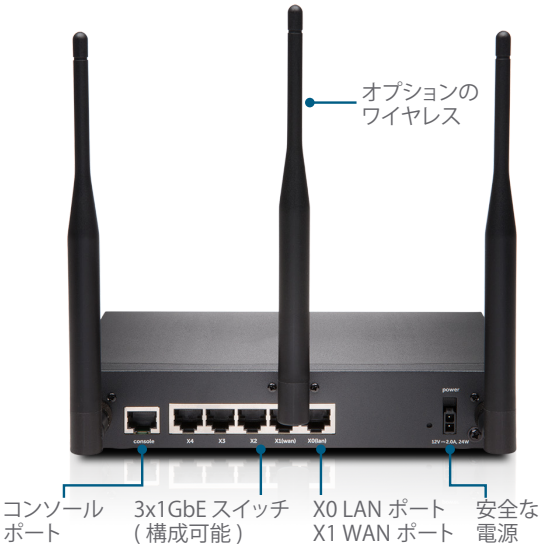
仕様	TZ400 シリーズ
ファイアウォールのスループット	1.3 Gbps
フル DPI のスループット	300 Mbps
マルウェア対策のスループット	300 Mbps
IPS スループット	900 Mbps
IMIX スループット	500 Mbps
DPI 最大接続数	90,000
新規接続数 / 秒	6,000



SonicWall TZ300 シリーズ

SonicWall TZ300 シリーズは、ネットワークを攻撃から保護するオールインワンのソリューションを提供します。コンシューマクラスの製品とは異なり、SonicWall TZ300 シリーズのファイアウォールは、効果的な侵入防御、マルウェア対策、コンテンツ /URL フィルタリングを組み合わせ、さらにオプションの 802.11ac 内蔵ワイヤレスを加えることで、ノートパソコン、スマートフォン、タブレット用プラットフォームを最も幅広くサポートしています。

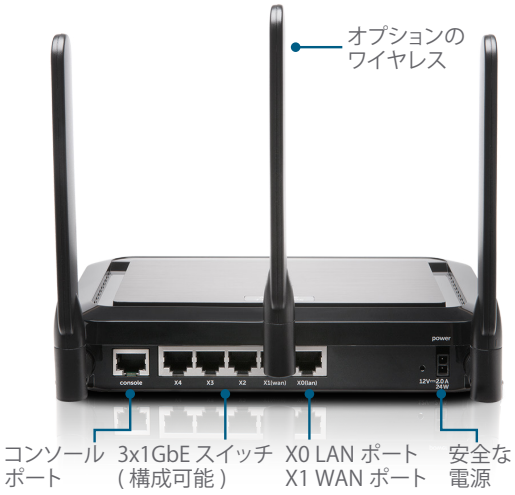
仕様	TZ300 シリーズ
ファイアウォールのスループット	750 Mbps
フル DPI のスループット	100 Mbps
マルウェア対策のスループット	100 Mbps
IPS スループット	300 Mbps
IMIX スループット	200 Mbps
DPI 最大接続数	50,000
新規接続数 / 秒	5,000



SonicWall SOHO シリーズ

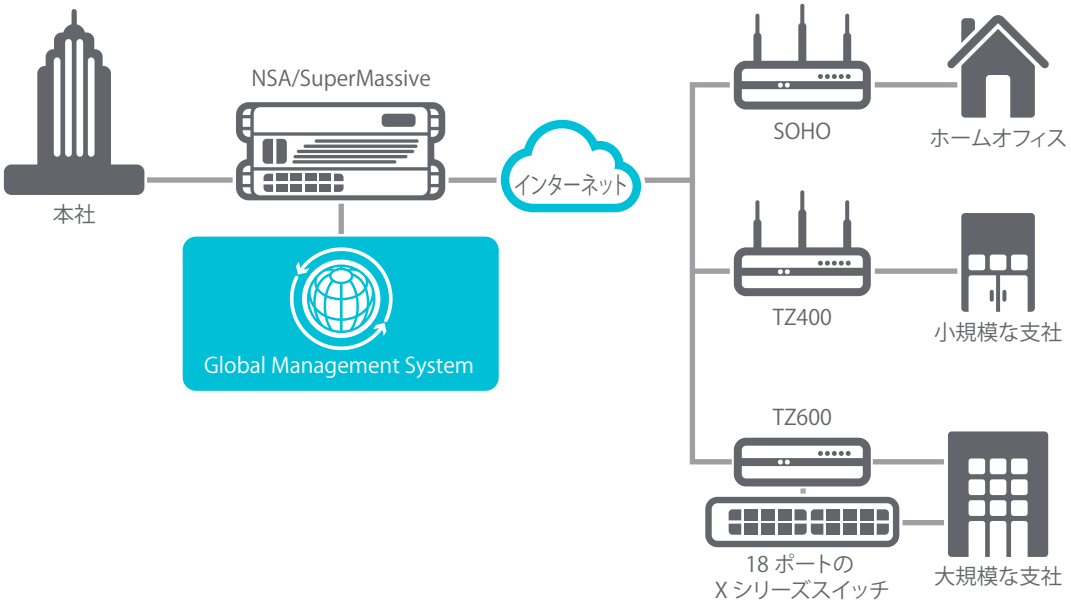
有線およびワイヤレスで接続するスモールオフィスやホームオフィス環境のための SonicWall SOHO シリーズは、大規模組織と同様のビジネスクラスの保護を、より低価格で提供します。

仕様	SOHO シリーズ
ファイアウォールのスループット	300 Mbps
フル DPI のスループット	50 Mbps
マルウェア対策のスループット	50 Mbps
IPS スループット	100 Mbps
IMIX スループット	60 Mbps
DPI 最大接続数	10,000
新規接続数 / 秒	1,800



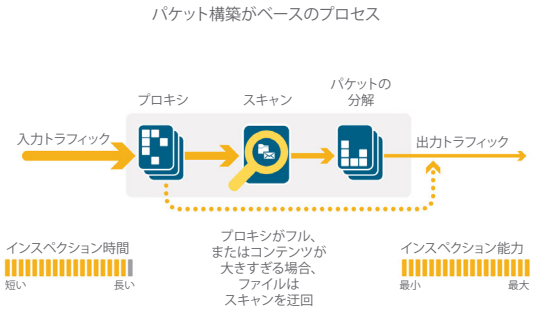
優れた拡張性とパフォーマンスを実現する拡張可能なアーキテクチャ

再構築不要のディープ・パケット・インスペクション (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行うことを重視して、一から設計されており、本質的に並列で発生し、増加し続ける性質のネットワークトラフィックに適しています。マルチコアのプロセッサーシステムと組み合わされて並列処理を実行するソフトウェアアーキテクチャにより、高負荷のトラフィックにおけるディープ・パケット・インスペクションの要求にも申し分なく応えることができます。SonicWall TZ シリーズのプラットフォームでは、x86 プロセッサーと異なり、パケット処理、暗号化通信処理、およびネットワーク処理に最適化された専用のプロセッサーを使用しています。そのため、ユーザーのネットワーク環境において、柔軟性とプログラム制御可能性を維持できます。これは ASIC システムにはない長所です。この柔軟性は、最新の高度な検知技術で対処する必要があ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非常に重要になります。

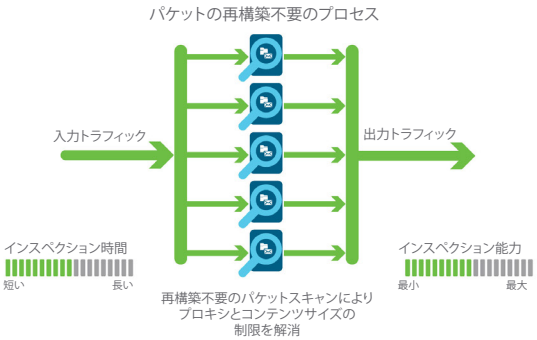


再構築不要のディープ・パケット・インスペクション（RFDPI）エンジン

RFDPI エンジンは、パフォーマンスを低下させずに優れた脅威対策やアプリケーション制御を提供します。特許取得済みのエンジンが、トラフィックストリームを検査することでレイヤ 3 ～ 7 での脅威を検知します。ネットワークストリームに大規模な正規化と復号化を繰り返し行い、検知エンジンを混乱させネットワークに悪意あるコードをまぎれこませようとする高度な回避技術を、RFDPI エンジンが無効にします。パケットは SSL 復号化などの必要な前処理を受けた後で、侵入攻撃、マルウェア、および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合わせて分析されます。次に、これらのデータベースに対応する位置まで接続状態が進められ、その位置が攻撃状態またはその他の「一致」イベントの状態と一致すると、事前に設定されたアクションが実行されます。マルウェアが特定されると、SonicWall ファイアウォールは、何らかの侵害が行われる前に接続を切り、イベントを適切に記録します。ただし、エンジンを検知専用に設定することや、アプリケーション検知の場合に、アプリケーションが識別されたらすぐアプリケーションストリームの残りについてレイヤ 7 帯域幅管理サービスを提供するように設定することもできます。



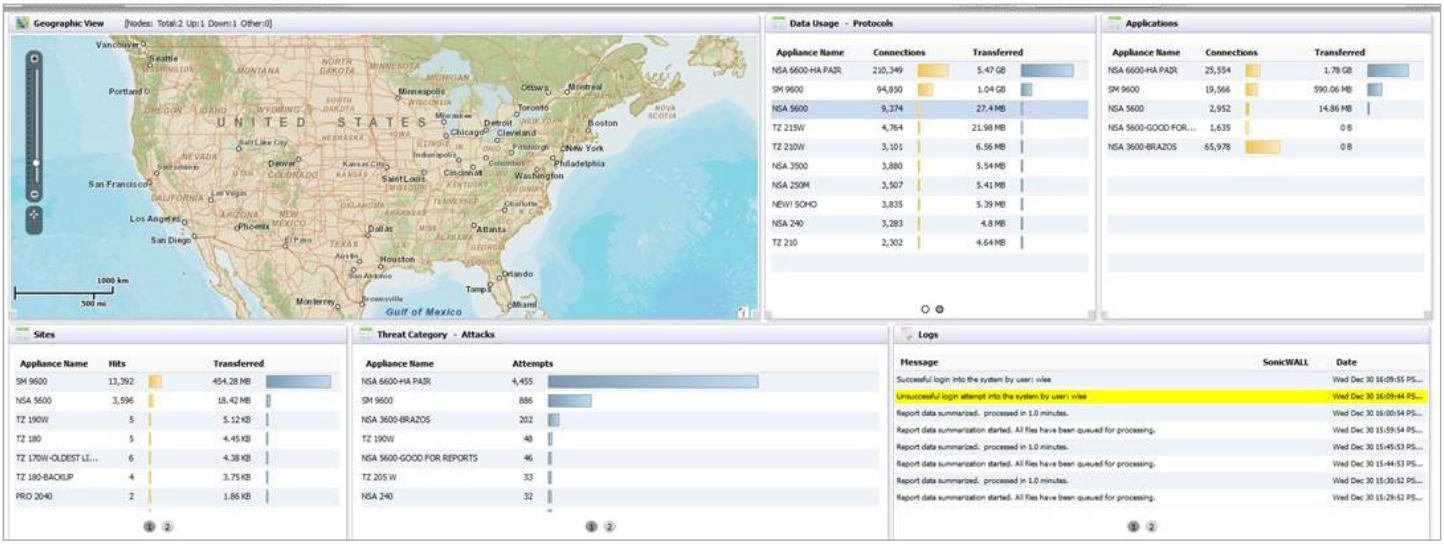
競合アーキテクチャ



SonicWall アーキテクチャ

グローバルな管理およびレポート機能

大規模な分散型企業に展開する場合、オプションの SonicWall Global Management System (GMS) を利用することで、管理者は統合された安全で包括的なプラットフォームを使用して SonicWall のセキュリティアプライアンスと X シリーズスイッチを管理できます。GMS によって管理者はセキュリティアプライアンスの管理を簡単に集約することができ、管理やトラブルシューティングに伴う煩雑な業務を削減できます。さらに、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運用に求められるあらゆる側面をカバーできます。GMS はほかにも、ワークフローの自動化機能によって、エンタープライズでのファイアウォールの変更管理要件に応えることもできます。GMS は、ビジネスプロセスやサービスレベルごとのネットワークセキュリティ管理に最適です。管理はデバイス単位ではなく、セキュリティ環境全体にフォーカスしているので、ライフサイクル管理を劇的に簡素化できます。

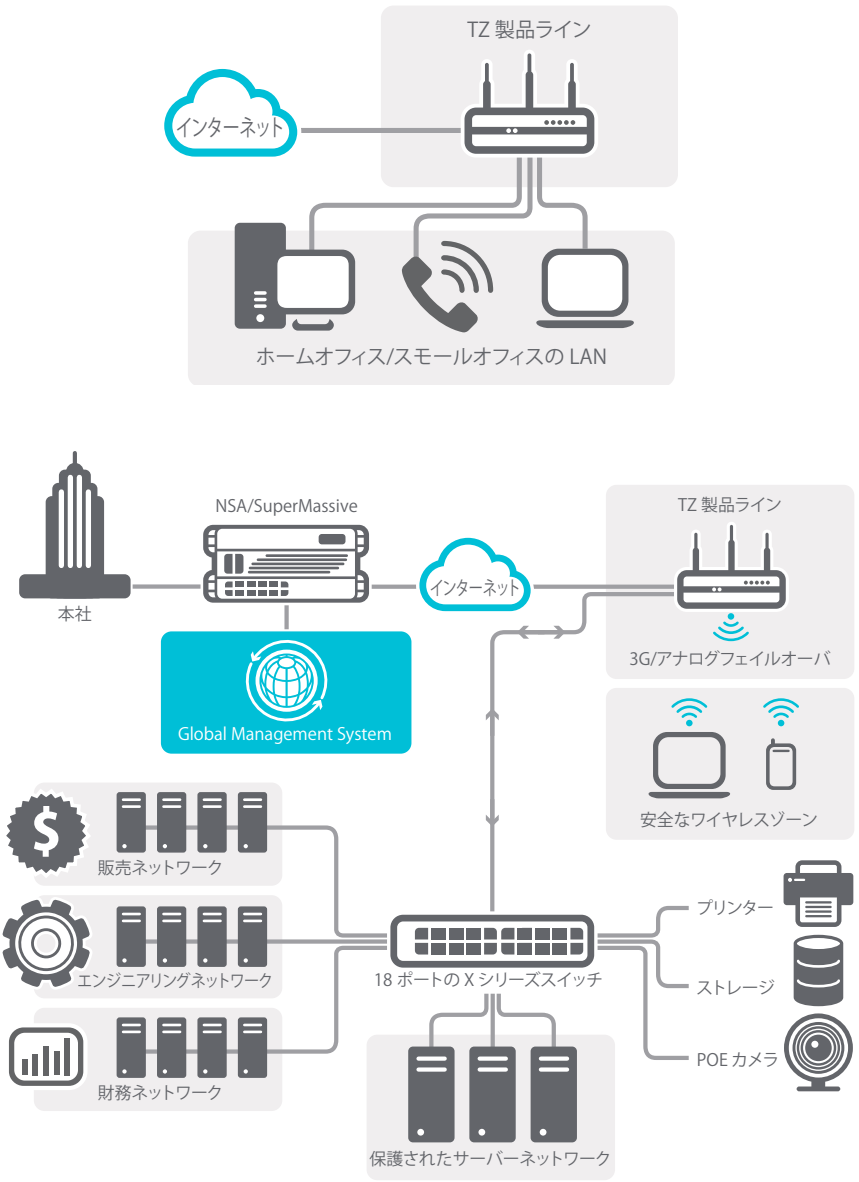


セキュリティと保護

SonicWall では専従の脅威調査チームが最新の保護を実現するために現場にファイアウォールに導入する防衛策の研究と開発にあたっています。脅威調査チームは世界中の 100 万以上のセンサを活用してマルウェアのサンプルや最新の脅威情報についてのテレメトリフィードバックを入手し、これらを侵入防御、マルウェア対策、およびアプリケーション検知機能に生かしています。最新のサブスクリプションを持つ SonicWall ファイアウォールのお客様には、24 時間体制で常に更新される脅威防御が提供され、更新内容はリブートや中断なしに即座に有効になります。アプライアンスに保存されているシグネチャはさまざまな分野の攻撃を防御するように設計されており、1 つのシグネチャで何万もの異なる脅威に対応します。アプライアンスに組み込まれている防衛策に加えて、すべての SonicWall ファイアウォールは 1,700 万以上ものシグネチャ情報を保存し、さらに増加を続ける SonicWall CloudAV サービスにもアクセスできます。これにより、アプライアンス上のシグネチャインテリジェンスがさらに強化されます。この CloudAV データベースは、ファイアウォールから専用の軽量プロトコル経由でアクセスされ、アプライアンスで行うインスペクションを補強します。SonicWall の次世代ファイアウォールは Geo-IP およびボットネットフィルタリング機能があるため、危険なドメインからのトラフィックや、ある地域全体からのトラフィックをブロックして、ネットワーク上のリスクプロファイルを削減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 & コントロール

アプリケーションインテリジェンスにより、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ついて情報を得ることができ、ビジネスの優先順位を基にアプリケーションコントロールをスケジュール設定したり、非生産的なアプリケーションを抑制したり、潜在的な危険のあるアプリケーションをブロックしたりできます。リアルタイムな可視化によってトラフィックに異常が起きた時点でその異常を特定し、潜在的なインバウンド / 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措置を講じることができます。SonicWall アプリケーショントラフィック分析では、アプリケーショントラフィックや帯域幅利用、およびセキュリティの脅威を詳細に確認でき、また強力なトラブルシューティングやフォレンジック分析も可能になります。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が向上し、生産性が上がると同時に、サポートコールを減らすこともできます。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 & コントロールの管理をシンプルにします。



柔軟でセキュアなワイヤレス

オプション機能として利用可能な 802.11ac ワイヤレス* を SonicWall の次世代ファイアウォールテクノロジーと組み合わせることで、有線および無線のネットワークに総合的な保護を提供するワイヤレスのネットワーク・セキュリティ・ソリューションを構成します。

このエンタープライズレベルのワイヤレスパフォーマンスにより、離れた場所にある Wi-Fi 対応デバイスからの接続や、大きな帯域幅を必要とするモバイルアプリ (動画や音声など) の使用や、接続数の多い環境下の使用においても、信号の劣化が起こりにくくなります。

** 802.11ac は現在 SOHO モデルでは利用できません。SOHO モデルでは 802.11a/b/g/n をサポートしています。*

各種機能

RFDPI エンジン	
機能	説明
Reassembly-Free Deep Packet Inspection (再構築不要のディープ・パケット・インスペクション)	ハイパフォーマンスの専用インスペクションエンジン (特許取得済み) 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、プロキシ化またはバッファリングなしに侵入の試行やマルウェアを検出し、あらゆる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	送信トラフィックと受信トラフィックの両方で同時に脅威をスキャンするため、ネットワークがマルウェアの配布に利用されたり、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土台になったりするのを防止できます。
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、マルウェアや侵入のスキャンとアプリケーションの識別を同時に行います。このため、DPI の遅延を劇的に低減し、単一のアーキテクチャですべての脅威情報を確実に相互に関連付けることができます。
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ため、同時ネットワークストリームに対して超低遅延のディープ・パケット・インスペクション (DPI) を実現できます。ファイルやストリームのサイズに制限はなく、一般的なプロトコルだけでなく Raw TCP ストリームにも適用できます。
Capture による高度な脅威対策	
マルチエンジンサンドボックス	仮想サンドボックス、フル・システム・エミュレーション、およびハイパーバイザレベルの分析テクノロジーが搭載されたマルチエンジン・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、動作を分析して、悪意のあるアクティビティに対する包括的な可視性を提供します。
幅広い種類のファイルの分析	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 などの広範な種類のファイルに加えて、Windows、Android、Mac OSX、およびマルチブラウザ環境を含む複数のオペレーティングシステムの分析をサポートします。
シグネチャの迅速な展開	ファイルが不正であると特定されると、SonicWALL Capture サブスクリプションによってシグネチャがただちにファイアウォールへ導入され、GRID のゲートウェイアンチウイルスおよび IPS シグネチャデータベースと、URL、IP、およびドメインのレピュテーションデータベースに、48 時間以内に追加されます。
正体が判明するまでブロック	脅威となり得るファイルがネットワークに侵入しないよう、分析対象としてクラウドサービスに送られたファイルは、正体が判明するまでゲートウェイで保留にしておくことができます。
侵入防御	
機能	説明
防衛策ベースの保護	緊密に統合された侵入防御システム (IPS) では、シグネチャやその他の防衛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、幅広い種類の攻撃や脆弱性をカバーします。
シグネチャの自動更新	SonicWall の脅威調査チームは絶えず脅威を研究し、50 種類以上の攻撃分野をカバーする IPS のさまざまな防衛策リストを継続して更新しています。更新された防衛策は、リブートやサービスの中断をすることなく、ただちに適用されます。
ゾーン内での IPS 保護	侵入防御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散しないように防御することで、内部セキュリティを補強します。
ボットネットによるコマンドおよびコントロール (CnC) の検知およびブロック	マルウェアの拡散元または既知の CnC ポイントであると特定された IP やドメインに対して、ローカルネットワークに存在するボットが CnC トラフィックを送信しようとするのを検知し、その通信をブロックします。
プロトコル違反 / 異常	IPS による防御をすり抜けようと、プロトコルを不正に使用する攻撃を検知し、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が利用する最新の手口やテクニックに対抗できるよう常に更新されているので、ゼロデイ攻撃からもネットワークを保護できます。
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 で検知回避技術を利用した脅威がネットワークに侵入を試みても、侵入の前に検知することができます。
脅威防御	
機能	説明
ゲートウェイでのマルウェア対策	RFDPI エンジンは、受信トラフィック、送信トラフィック、およびゾーン間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、およびその他のマルウェアがファイルにないかスキャンします。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 のマルウェア対策	SonicWall のクラウドサーバーには、1,700 万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、その内容は常に更新され続けています。搭載されているシグネチャデータベースはこのクラウドデータベースを参照することで機能を強化し、RFDPI でカバーできる脅威の数をさらに広げることができます。
常時セキュリティ更新	新しい脅威の更新は、セキュリティサービスを有効にしている現場のファイアウォールに自動的に送信され、リブートや中断することなく即座に有効になります。
SSL の復号化と検査	SSL トラフィックを復号化して、マルウェア、侵入、データ漏洩がないかをプロキシ化せずにその場で検査します。また、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からも保護します。SOHO を除いたすべてのモデルのセキュリティサブスクリプションに含まれます。SOHO モデルでは別途ライセンスとして販売されます。
双方向 Raw TCP インスペクション	RFDPI エンジンはあらゆるポートで Raw TCP ストリームを双方向からスキャンできるため、いくつかのウェルノウンポートしか保護しない旧式のセキュリティシステムでは見逃してしまう脅威であっても、侵入を許しません。
広範なプロトコルサポート	HTTP/S、FTP、SMTP、SMBv1/v2 など、Raw 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。

アプリケーションインテリジェンス & 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、常に更新を続ける 3,500 以上のアプリケーションシグネチャを格納したデータベースを参照することで、アプリケーションやアプリケーションの個々の機能をコントロールして、ネットワークセキュリティを強化しつつネットワーク生産性を向上させます。
カスタムアプリケーションの識別	特定のパラメータや、ネットワークにおけるアプリケーション固有の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コントロールしてネットワークの制御を強化します。
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やアプリケーションカテゴリに帯域幅を割り当てたり、重要度の低いアプリケーションのトラフィックを規制したりして、アプリケーションの帯域幅をきめ細かく調整します。
詳細なコントロール	LDAP/AD/ ターミナルサービス /Citrix 統合を利用した 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、さまざまなアクションに応じて、アプリケーションやアプリケーションの特定コンポーネントをコントロールします。
コンテンツフィルタリング	
機能	説明
内部および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・サービスを利用して、使用許諾ポリシーを適用し、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。Content Filtering Client によってポリシーの適用範囲を拡大し、ファイアウォール境界の外にあるデバイスがインターネットコンテンツにアクセスするのをブロックできます。
詳細なコントロール	事前定義されたカテゴリや、カテゴリの組み合わせを指定してコンテンツをブロックします。フィルタリングは授業時間中や営業時間中といった時間帯ごとに設定できるほか、個々のユーザーやグループに対して適用することもできます。
YouTube for Schools	教師は YouTube EDU にアップロードされている無数のビデオから学習用の無料動画を選べます。ビデオは科目や学年ごとに分けられ、一般的な教育基準にそって分類されています。
Web キャッシュ	URL のレーティングは SonicWall ファイアウォールのローカルにキャッシュされるので、頻繁に訪問するサイトへの後続のアクセスには一瞬で応答が返されます。
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	境界保護の最初のレイヤとしてファイアウォール機能を活用し、エンドポイント保護と組み合わせることで、ノートパソコン、USB メディア、およびその他の保護されていないシステムからネットワークにウイルスが侵入するのを防ぎます。
自動適用オプション	ネットワークにアクセスするすべてのコンピューターに、最新バージョンのウイルス対策とスパイウェア対策のシグネチャを確実にインストールし有効化します。これにより、通常であればデスクトップのウイルス対策とスパイウェア対策の管理にかかるコストをカットできます。
自動化された展開とインストールのオプション	ウイルス対策およびスパイウェア対策クライアントのインストールと展開は、ネットワーク全体でマシンごとに自動化されているので、管理業務のオーバーヘッド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	ウイルス対策とスパイウェア対策が頻繁に更新され、すべてのデスクトップとファイルサーバーにシームレスに適用されるため、ユーザーの生産性を高めると同時に、セキュリティ管理業務を減らすことができます。
スパイウェア検出	強力なスパイウェア対策保護が多様なスパイウェアプログラムを検出し、デスクトップやノートパソコンにインストールされて機密情報を送信される前に、そのスパイウェアをブロックします。これにより、デスクトップのセキュリティとパフォーマンスが大幅に高まります。
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および分析し、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 攻撃からの防御	SYN Flood 防御は、レイヤ 3 SYN プロキシおよびレイヤ 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 Flood 防御および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。
柔軟な展開オプション	SonicWall TZ 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・モードで展開できます。
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 では、ハードウェアでフィルタリング実装をサポートします。
X シリーズスイッチ統合	X シリーズスイッチとの統合により、TZ シリーズダッシュボードを使用して POE および POE+ を含む追加のポートのセキュリティ設定を一元的に管理できます (SOHO モデルでは利用不可)。
高可用性	SonicWall TZ500 および SonicWall TZ600 モデルは、ステート同期による Active/Standby が有効な高可用性をサポートしています。SonicWall TZ300 および SonicWall TZ400 モデルは、Active/Standby 同期が無効な高可用性をサポートしています。SonicWall SOHO モデルには高可用性機能はありません。
ワイヤレスネットワークのセキュリティ	IEEE 802.11ac ワイヤレステクノロジーは、最高 1.3 Gbps のワイヤレススループットにより、より広範囲の信頼性を実現しました。SonicWall TZ600 から SonicWall TZ300 モデルでご利用いただけます。オプションの 802.11 a/b/g/n は、SonicWall SOHO モデルでご利用いただけます。
管理およびレポート機能	
機能	説明
Global Management System	SonicWall の 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から複数の SonicWall アプライアンスと X シリーズスイッチを監視、構成、およびレポート作成できるので、管理コストや複雑さを軽減できます。
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、迅速で簡単な構成が可能です。また、包括的なコマンド・ライン・インターフェイスと 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 や NetFlow のプロトコルを使用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て、リアルタイム監視と履歴監視を行ったり、SonicWall Scrutinizer やその他の拡張 IPFIX/NetFlow 対応のツールを使用してレポートを作成したりできます。

仮想プライベートネットワーク	
機能	説明
サイト間接続型 IPSec VPN	ハイパフォーマンスの IPSec VPN により、SonicWall TZ シリーズは他の何千という大規模なサイト、支店、本店を接続する VPN コンセントレータとして機能できます。
SSL VPN または IPSec クライアント・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しやすい IPSec クライアントを利用して、E 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、さまざまなプラットフォームから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、プライマリ VPN とセカンダリ VPN を構成して、すべての VPN セッションを自動かつシームレスにフェイルオーバおよびフェイルバックできます。
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する機能によって、エンドポイント間で代替ルート経由でトラフィックをシームレスに再ルーティングし、一時的な VPN トンネル障害時も確実にアップタイムを維持できます。
コンテキスト / 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は、シームレスな AD/LDAP/Citrix1/ ターミナルサービス SSO 統合および DPI を通じて取得された広範な情報により追跡可能になります。
GeoIP 国別のトラフィック識別	特定の国へ、または特定の国からのトラフィックを識別してコントロールし、既知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およびコントロールして、データ漏洩を防ぎます。

SonicOS 機能の概要

ファイアウォール

- Reassembly-Free Deep Packet Inspection (再構築不要のディープ・パケット・インスペクション)
- ディープ・パケット・インスペクション (SSL)
- 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) サポート
- DOS 攻撃からの防御
- UDP/ICMP/SYN Flood 防御
- SSL 復号化

Capture ATP:

- クラウドベースのマルチエンジン分析
- 仮想化サンドボックス
- 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
- 幅広い種類のファイルの検査
- 自動および手動による提出
- 脅威インテリジェンスのリアルタイム更新
- 自動ブロック機能

侵入防御

- シグネチャベースのスキャン
- シグネチャの自動更新
- 双方向のインスペクションエンジン
- 詳細な IPS ルール機能
- 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

マルウェア対策

- 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
- 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
- 帯域幅管理 CFS 評価カテゴリ
- 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
- 57 種類のコンテンツ・フィルタリング・カテゴリ

VPN

- サイト間接続型 IPSec VPN
- SSL VPN および IPSec クライアント・リモート・アクセス
- 冗長 VPN ゲートウェイ
- Mobile Connect for iOS and Android™
- ルートベース VPN (OSPF、RIP)

ネットワーク

- PortShield
- レイヤ 2 のネットワーク検出
- 強化されたログ機能
- ポートミラーリング
- レイヤ 2 の QoS
- ポートセキュリティ
- ダイナミックルーティング
- ポリシーベースのルーティング
- 非対称ルーティング
- DHCP サーバー
- 帯域幅の管理
- ステートシンクによる Active/Standby 高可用性 *
- 受信 / 送信トラフィックの負荷バランシング
- L2 ブリッジ、NAT モード DDNS
- 3G/4G WAN フェイルオーバ
- **VoIP**
- 詳細な QoS コントロール
- 帯域幅の管理
- 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
- 集中化された管理とレポート
- ログ記録
- Netflow/IPFix エクスポート
- アプリケーショントラフィックの可視化 (SOHO モデルでは利用不可)
- ポリシーの一元管理
- シングルサインオン (SSO)
- ターミナルサービス /Citrix サポート
- アプリケーションと帯域幅の可視化
- IPv4 と IPv6 の管理

IPv6

- IPv6 フィルタリング
- 6rd (迅速な導入)
- DHCP Prefix Delegation
- BGP

ワイヤレス

- デュアルバンド (2.4 GHz および 5.0 GHz)
- 802.11 a/b/g/n/ac ワイヤレス標準 **
- ワイヤレスの侵入検出および保護機能
- ワイヤレスゲストサービス
- ライトウエイト・ホットスポット・メッセージング
- 仮想アクセスポイントの区分
- キャプティブポータル
- クラウド ACL

** ステートシンクの高可用性は SonicWall TZ500 および SonicWall TZ600 モデルのみ利用可能*
*** 802.11ac は SOHO モデルでは利用不可*
**** Geo-IP およびボットネットフィルタは SOHO シリーズモデルでは利用不可*

SonicWall TZ シリーズのシステム仕様

パフォーマンスの概要	SOHO シリーズ	TZ300 シリーズ	TZ400 シリーズ	TZ500 シリーズ	TZ600 シリーズ
オペレーティングシステム	SonicOS 5.9x / 6.2.x	SonicOS 6.2.x			
セキュリティプロセッサー	2 x 400 MHz / 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1.4 GHz
メモリ (RAM)	512 MB / 1 GB	1 GB	1 GB	1 GB	1 GB
メモリ (フラッシュ)	32 MB / 64 MB	64 MB	64 MB	64 MB	64 MB
1 GbE 銅線インターフェイス	5	5	7	8	10
拡張	USB	USB	USB	USB x 2	拡張スロット (背面)*、USB x 2
ファイアウォールインスペクションのスループット [1]	300 Mbps	750 Mbps	1,300 Mbps	1,400 Mbps	1,500 Mbps
フル DPI のスループット [2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
アプリケーションインスペクションのスループット [2]	-	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
IPS のスループット [2]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
マルウェア対策インスペクションのスループット [2]	50 Mbps	100 Mbps	300 Mbps	400 Mbps	500 Mbps
IMIX のスループット [3]	60 Mbps	200 Mbps	500 Mbps	700 Mbps	900 Mbps
SSL インスペクションと復号化スループット (DPI SSL)[2]	15 Mbps	45 Mbps	100 Mbps	150 Mbps	200 Mbps
IPSec VPN のスループット [3]	100 Mbps	300 Mbps	900 Mbps	1,000 Mbps	1,100 Mbps
接続数 / 秒	1,800	5,000	6,000	8,000	12,000
最大接続数 (SPI)	10,000	50,000	100,000	125,000	150,000
最大接続数 (DPI)	10,000	50,000	90,000	100,000	125,000
シングルサインオン (SSO) ユーザー数	250	500	500	500	500
VLAN インターフェイス	25	25	50	50	50
SonicPoint サポート数 (最大)	2	8	16	16	24
サポートされる X シリーズ・スイッチ・モデル	利用不可	X1008/P、X1018/P、X1026/P、X1052/P、X4012			
VPN	**SOHO シリーズ**	**TZ300 シリーズ**	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
サイト間 VPN トンネル	10	10	20	25	50
IPSec VPN クライアント (最大)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL VPN ライセンス数 (最大)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Virtual Assist 同梱数 (最大)	-	1 (30 日間評価版)	1 (30 日間評価版)	1 (30 日間評価版)	1 (30 日間評価版)
暗号化 / 認証	DES、3DES、AES (128、192、256 ビット)、MD5、SHA-1、Suite B 暗号化				
キー交換	Diffie Hellman グループ 1、2、5、14				
ルートベース VPN	RIP、OSPF				
証明書のサポート	Verisign、Thawte、Cybertrust、RSA Keon、Entrust、SonicWall から SonicWall VPN への認定を行う Microsoft CA、SCEP				
VPN 機能	Dead Peer Detection、DHCP Over VPN、IPSec NAT トラバーサル、冗長 VPN ゲートウェイ、ルートベース VPN				
サポートされているグローバル VPN クライアントプラットフォーム	Microsoft® Windows Vista 32/64 ビット、Windows 7 32/64 ビット、Windows 8.0 32/64 ビット、Windows 8.1 32/64 ビット、Windows 10				
NetExtender	Microsoft Windows Vista 32/64 ビット、Windows 7、Windows 8.0 32/64 ビット、Windows 8.1 32/64 ビット、Mac OS X 10.4 以上、Linux FC3 以上 /Ubuntu 7 以上 /OpenSUSE				
Mobile Connect	Apple® iOS、Mac OS X、Google® Android™、Kindle Fire、Windows 8.1 (Embedded)				
セキュリティサービス	**SOHO シリーズ**	**TZ300 シリーズ**	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
ディープ・パケット・インスペクション・サービス	ゲートウェイアンチウイルス、アンチスパイウェア、侵入防御、DPI SSL				
コンテンツ・フィルタリング・サービス (CFS)	HTTP URL、HTTPS IP、キーワードとコンテンツのスキャン、ActiveX、Java、プライバシーの Cookie などファイルの種類に基づく包括的なフィルタリング、および許可 / 拒否リスト				
エンフォースド・クライアント・アンチウイルス / アンチスパイウェア	McAfee®				
Comprehensive Anti-Spam Service	サポート対象				
アプリケーションの可視化	いいえ	はい	はい	はい	はい
アプリケーションコントロール	はい	はい	はい	はい	はい
Capture による高度な脅威対策	いいえ	はい	はい	はい	はい

SonicWall TZ シリーズのシステム仕様 (続き)

ネットワーク	SOHO シリーズ	TZ300 シリーズ	TZ400 シリーズ	TZ500 シリーズ	TZ600 シリーズ
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				
NAT モード	1 対 1、1 対多、多対 1、多対多、フレキシブル NAT (重複 IP)、PAT、トランスペアレントモード				
ルーティングプロトコル [4]	BGP[4]、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング、マルチキャスト				
QoS	帯域幅の優先度、最大帯域幅、帯域幅保証、DSCP マーキング、802.1e (WMM)				
認証	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザーデータベース	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			
ローカル・ユーザー・データベース	150			250	
VoIP	フル H.323v1-5、SIP				
標準	TCP/IP、UDP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3				
認定資格	FIPS 140-2 (Suite B) Level 2、UC APL、VPNC、IPv6 (フェーズ 2)、ICSA ネットワークファイアウォール、ICSA ウイルス対策				
認定審査中	コモンクライテリア (NDPP)				
Common Access Card (CAC)	サポート対象				
高可用性	いいえ	Active/Standby	Active/Standby	ステートフル同期による Active/Standby	ステートフル同期による Active/Standby
ハードウェア	**SOHO シリーズ**	**TZ300 シリーズ**	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
フォームファクタ	デスクトップ				
PSU (W)	24W (外付)	24W (外付)	24W (外付)	36W (外付)	60W (外付)
最大消費電力 (W)	6.4 / 11.3	6.9 / 12.0	9.2 / 13.8	13.4 / 17.7	16.1
入力電源	100 ～ 240 VAC、50 ～ 60 Hz、1 A				
総発熱量	21.8 / 38.7 BTU	23.5 / 40.9 BTU	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
寸法	3.6x14.1x19cm	3.5x13.4x19cm	3.5x13.4x19cm	3.5x15x22.5cm	3.5x18x28cm
重量	0.34 kg / 0.75 ポンド 0.48 kg / 1.06 ポンド	0.73 kg / 1.61 ポンド 0.84 kg / 1.85 ポンド	0.73 kg / 1.61 ポンド 0.84 kg / 1.85 ポンド	0.92 kg / 2.03 ポンド 1.05 kg / 2.31 ポンド	1.47 kg / 3.24 ポンド
WEEE 重量	0.80 kg / 1.76 ポンド 0.94 kg / 2.07 ポンド	1.15 kg / 2.53 ポンド 1.26 kg / 2.78 ポンド	1.15 kg / 2.53 ポンド 1.26 kg / 2.78 ポンド	1.34 kg / 2.95 ポンド 1.48 kg / 3.26 ポンド	1.89 kg / 4.16 ポンド
出荷時の重量	1.20 kg / 2.64 ポンド 1.34 kg / 2.95 ポンド	1.37 kg / 3.02 ポンド 1.48 kg / 3.26 ポンド	1.37 kg / 3.02 ポンド 1.48 kg / 3.26 ポンド	1.93 kg / 4.25 ポンド 2.07 kg / 4.56 ポンド	2.48 kg / 5.47 ポンド
MTBF (年)	30/15	28/14	27/13	20/12	18
環境	0 ～ 40° C (40 ～ 105° F)				
湿度	5 ～ 95% （結露しないこと）				
規制	**SOHO シリーズ**	**TZ300 シリーズ**	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
法令遵守モデル (有線)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
主要な法令の遵守 (有線モデル)	FCC クラス B、ICES クラス B、CE (EMC、LVD、RoHS)、C-Tick、VCCI クラス B、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH、KCC/MSIP	FCC クラス B、ICES クラス B、CE (EMC、LVD、RoHS)、C-Tick、VCCI クラス B、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH、KCC/MSIP	FCC クラス B、ICES クラス B、CE (EMC、LVD、RoHS)、C-Tick、VCCI クラス B、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH、KCC/MSIP	FCC クラス B、ICES クラス B、CE (EMC、LVD、RoHS)、C-Tick、VCCI クラス B、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH、BSMI、KCC/MSIP	FCC クラス A、ICES クラス A、CE (EMC、LVD、RoHS)、C-Tick、VCCI クラス A、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH、KCC/MSIP
法令遵守モデル (ワイヤレス)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
主要な法令の遵守 (ワイヤレスモデル)	FCC クラス B、FCC RF ICES クラス B、IC RF CE (R&TTE、EMC、LVD、RoHS)、RCM、VCCI クラス B、MIC/TELEC、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH	FCC クラス B、FCC RF ICES クラス B、IC RF CE (R&TTE、EMC、LVD、RoHS)、RCM、VCCI クラス B、MIC/TELEC、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH	FCC クラス B、FCC RF ICES クラス B、IC RF CE (R&TTE、EMC、LVD、RoHS)、RCM、VCCI クラス B、MIC/TELEC、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH	FCC クラス B、FCC RF ICES クラス B、IC RF CE (R&TTE、EMC、LVD、RoHS)、RCM、VCCI クラス B、MIC/TELEC、UL、cUL、TUV/GS、CB、UL によるメキシコ CoC、WEEE、REACH	-

SonicWall TZ シリーズのシステム仕様 (続き)

内蔵ワイヤレス	SOHO シリーズ	TZ300、TZ400、TZ500 シリーズ	TZ600 シリーズ
標準	802.11 a/b/g/n	802.11a/b/g/n/ac (WEP、WPA、WPA2、802.11i、TKIP、PSK,02.1x、EAP-PEAP、EAP-TTLS)	-
周波数帯 [5]	802.11a: 5.180-5.825 GHz、802.11b/g: 2.412-2.472 GHz、802.11n: 2.412-2.472 GHz、5.180-5.825 GHz	802.11a: 5.180-5.825 GHz、802.11b/g: 2.412-2.472 GHz、802.11n: 2.412-2.472 GHz、5.180-5.825 GHz、802.11ac: 2.412-2.472 GHz、5.180-5.825 GHz	-
動作するチャネル	802.11a: 米国およびカナダ 12、欧州 11、日本 4、シンガポール 4、台湾 4、802.11b/g: 米国およびカナダ 1 ～ 11、欧州 1 ～ 13、日本 1 ～ 14 (14-802.11b のみ)、802.11n (2.4 GHz): 米国およびカナダ 1 ～ 11、欧州 1 ～ 13、日本 1 ～ 13、802.11n (5 GHz): 米国およびカナダ 36 ～ 48/149 ～ 165、欧州 36 ～ 48、日本 36 ～ 48、スペイン 36 ～ 48/52 ～ 64	802.11a: 米国およびカナダ 12、欧州 11、日本 4、シンガポール 4、台湾 4、802.11b/g: 米国およびカナダ 1 ～ 11、欧州 1 ～ 13、日本 1 ～ 14 (14-802.11b のみ)、802.11n (2.4 GHz): 米国およびカナダ 1 ～ 11、欧州 1 ～ 13、日本 1 ～ 13、802.11n (5 GHz): 米国およびカナダ 36 ～ 48/149 ～ 165、欧州 36 ～ 48、日本 36 ～ 48、スペイン 36 ～ 48/52 ～ 64、802.11ac: 米国およびカナダ 36 ～ 48/149 ～ 165、欧州 36 ～ 48、日本 36 ～ 48、スペイン 36 ～ 48/52 ～ 64	-
送信出力電力	システム管理者が指定した規制区分に基づく	システム管理者が指定した規制区分に基づく	-
TPC (送信電力制御)	サポート対象	サポート対象	-
サポート対象データレート	802.11a: 6、9、12、18、24、36、48、54 Mbps/ チャネル、802.11b: 1、2、5.5、11 Mbps/ チャネル、802.11g: 6、9、12、18、24、36、48、54 Mbps/ チャネル、802.11n: 7.2、14.4、21.7、28.9、43.3、57.8、65、72.2、15、30、45、60、90、120、135、150 Mbps/ チャネル	802.11a: 6、9、12、18、24、36、48、54 Mbps/ チャネル、802.11b: 1、2、5.5、11 Mbps/ チャネル、802.11g: 6、9、12、18、24、36、48、54 Mbps/ チャネル、802.11n: 7.2、14.4、21.7、28.9、43.3、57.8、65、72.2、15、30、45、60、90、120、135、150 Mbps/ チャネル、802.11ac: 7.2、14.4、21.7、28.9、43.3、57.8、65、72.2、86.7、96.3、15、30、45、60、90、120、135、150、180、200、32.5、65、97.5、130、195、260、292.5、325、390、433.3、65、130、195、260、390、520、585、650、780、866.7 Mbps/ チャネル	-
変調技術	802.11a: 直交周波数分割多重方式 (OFDM)、802.11b: 直接スペクトラム拡散 (DSSS)、802.11g: 直交周波数分割多重方式 (OFDM)/ 直接スペクトラム拡散 (DSSS)、802.11n: 直交周波数分割多重方式 (OFDM)	802.11a: 直交周波数分割多重方式 (OFDM)、802.11b: 直接スペクトラム拡散 (DSSS)、802.11g: 直交周波数分割多重方式 (OFDM)/ 直接スペクトラム拡散 (DSSS)、802.11n: 直交周波数分割多重方式 (OFDM)、802.11ac: 直交周波数分割多重方式 (OFDM)	-

** 今後使用予定。*
[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および Ixia のテストツールを使用して測定しています。テストには、複数のポートペアに対する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、および在庫状況は、変更されることがあります。
[4] BGP は、SonicWall TZ400、TZ500、および TZ600 でのみ提供されます。
[5] すべて TZ 内蔵ワイヤレスモデルでは、2.4GHz または 5GHz の周波数帯のどちらかがサポートされます。デュアルバンドサポートには、SonicWall ワイヤレス・アクセス・ポイント製品 (SonicPoints) を使用してください。

SonicWall TZ シリーズの注文情報

製品	SKU
SonicWall SOHO + TotalSecure (1 年間)	01-SSC-0651
SonicWall SOHO Wireless-N + TotalSecure (1 年間)	01-SSC-0653
SonicWall TZ300 + TotalSecure (1 年間)	01-SSC-0581
SonicWall TZ300 Wireless-AC + TotalSecure (1 年間)	01-SSC-0583
SonicWall TZ400 + TotalSecure (1 年間)	01-SSC-0514
SonicWall TZ400 Wireless-AC + TotalSecure (1 年間)	01-SSC-0516
SonicWall TZ500 + TotalSecure (1 年間)	01-SSC-0445
SonicWall TZ500 Wireless-AC + TotalSecure (1 年間)	01-SSC-0446
SonicWall TZ600 + TotalSecure (1 年間)	01-SSC-0219
高可用性オプション (各ユニットは同じモデルであることが必要)	
SonicWall TZ500 高可用性	01-SSC-0439
SonicWall TZ600 高可用性	01-SSC-0220

SonicWall TZ シリーズの注文情報 (続き)

サービス	SKU
SonicWall SOHO 向け	
Comprehensive Gateway Security Suite (1 年間)	01-SSC-0688
ゲートウェイアンチウイルス、侵入防御、アプリケーションコントロール (1 年間)	01-SSC-0670
コンテンツ・フィルタリング・サービス (1 年間)	01-SSC-0676
Comprehensive Anti-Spam Service (1 年間)	01-SSC-0682
24x7 サポート (1 年間)	01-SSC-0700
SonicWall TZ300 向け	
Advanced Gateway Security Suite – Capture ATP、脅威防御、コンテンツフィルタリング、TZ300 の 24x7 サポート (1 年間)	01-SSC-1430
TZ300 の Capture による高度な脅威対策 (ATP) (1 年間)	01-SSC-1435
ゲートウェイアンチウイルス、侵入防御、アプリケーションコントロール (1 年間)	01-SSC-0602
コンテンツ・フィルタリング・サービス (1 年間)	01-SSC-0608
Comprehensive Anti-Spam Service (1 年間)	01-SSC-0632
24x7 サポート (1 年間)	01-SSC-0620
SonicWall TZ400 向け	
Advanced Gateway Security Suite – Capture ATP、脅威防御、コンテンツフィルタリング、TZ400 の 24x7 サポート (1 年間)	01-SSC-1440
TZ400 の Capture による高度な脅威対策 (ATP) (1 年間)	01-SSC-1445
ゲートウェイアンチウイルス、侵入防御、アプリケーションコントロール (1 年間)	01-SSC-0534
コンテンツ・フィルタリング・サービス (1 年間)	01-SSC-0540
Comprehensive Anti-Spam Service (1 年間)	01-SSC-0561
24x7 サポート (1 年間)	01-SSC-0552
SonicWall TZ500 向け	
Advanced Gateway Security Suite – Capture ATP、脅威防御、コンテンツフィルタリング、TZ500 の 24x7 サポート (1 年間)	01-SSC-1450
TZ500 の Capture による高度な脅威対策 (ATP) (1 年間)	01-SSC-1455
ゲートウェイアンチウイルス、侵入防御、アプリケーションコントロール (1 年間)	01-SSC-0458
コンテンツ・フィルタリング・サービス (1 年間)	01-SSC-0464
Comprehensive Anti-Spam Service (1 年間)	01-SSC-0482
24x7 サポート (1 年間)	01-SSC-0476
SonicWall TZ600 向け	
Advanced Gateway Security Suite – Capture ATP、脅威防御、コンテンツフィルタリング、TZ600 の 24x7 サポート (1 年間)	01-SSC-1460
TZ600 の Capture による高度な脅威対策 (ATP) (1 年間)	01-SSC-1465
ゲートウェイアンチウイルス、侵入防御、アプリケーションコントロール (1 年間)	01-SSC-0228
コンテンツ・フィルタリング・サービス (1 年間)	01-SSC-0234
Comprehensive Anti-Spam Service (1 年間)	01-SSC-0252
24x7 サポート (1 年間)	01-SSC-0246

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、電子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-SonicWall-TZ Series-US-VG-26141

SONICWALL™