Gartner peerinsights customers' choice 2018

SONICWALL

SonicWall TZ シリーズ

中小組織および分散型企業向けの統合脅威防御と SD-WAN プラットフォーム

SonicWall TZ シリーズは、小規模から中規模の組織、および分散型企業に、あらゆる要件を満たす統合セキュリティソリューションの利点をもたらします。高速の脅威防御、ソフトウェア定義ワイドエリアネットワーキング (SD-WAN) テクノロジー、幅広いネットワークとワイヤレスの機能、シンプルな導入と一元化された管理を組み合わせることによって、TZ シリーズは総所有コストを低く抑えた統合セキュリティソリューションを提供します。

柔軟で統合されたセキュリティソリューション

TZ シリーズの基盤は、SonicWall の機能豊富なオペレーティングシステムである SonicOS です。SonicOS には、これらの統合脅威管理 (UTM) ファイアウォールを個別のネットワーク要件に合わせて組織が柔軟に調整できるようにするための強力な機能セットが備わっています。たとえば、セキュアな高速ワイヤレスネットワークの構築は、内蔵ワイヤレスコントローラと IEEE 802.11ac 標準のサポートによって、また SonicWave 802.11ac Wave 2 アクセスポイントの追加によって簡素化されています。高速ワイヤレスアクセスポイント、およびその他の Power over Ethernet (PoE) 対応デバイス (IP カメラ、電話、プリンターなど) の接続時のコストと複雑性を軽減するために、TZ300P および TZ600P は、PoE/PoE+ 給電機能を備えています。

分散小売事業と現場環境では、SonicOS の多くのツールを活用して、より大きな利益を上げることができます。ブランチオフィスは、仮想プライベートネットワーキング (VPN) を使用して中央のオフィスと安全に情報を交換できます。仮想 LAN (VLAN) を作成することで、ネットワークを別々の企業グループおよび顧客グループにセグメント化して、他の VLAN のデバイスとの通信レベルを決定するルールを設定できます。SD-WAN はコストの高い MPLS 回路に代わる安全な代替機能を提供し、アプリケーションの性能と可用性に一貫性をもたらします。リモートロケーションに TZ ファイアウォールを導入することで、クラウドによるリモートでのファイアウォールのプロビジョニングを可能にするゼロタッチ導入を簡単に利用できます。

優れた脅威防御とパフォーマンス

サイバー脅威が絶えず進化し続けている現状において、ネットワークを保護するために弊社が必要と考えるのは、自動化されたリアルタイムの脅威の検出と防御です。弊社は、クラウドベースとオンボックスの両方のテクノロジーを組み合わせたファイアウォールの防御機能を提供しており、独立した第三者のテストによって、極めて高いセキュリティの有効性が認定されています。未知の脅威は、SonicWall のクラウドベースの Capture Advanced Threat Protection (ATP) マルチエンジンサンドボックスに送られて分析されます。Capture ATP を強化するのが、特許出願中の Real-Time Deep Memory Inspection (RTDMI™) テクノロジーです。RTDMI エンジンはメモリ内を直接検査することで、マルウェアとゼロデイ脅威を検出し、ブロックします。正確性に優れる RTDMI 技術は誤検出を最小限に抑制し、マルウェアの武器を検出できる時間が 100 ナノ秒にも満たない高度な攻撃を特定して軽減します。RTDMI と併用することで、弊社の特許取得済みシングルパス Reassembly-Free Deep Packet Inspection (RFDPI) エンジンは、すべてのパケットのすべてのバイトを調べて、インバウンドとアウトバウンドのトラフィックをファイアウォールで直接検査します。侵入防止、アンチマルウェア、Web/URL フィルタリングなどのオンボックス機能に加えて、SonicWall Capture Cloud Platform の Capture ATP と RTDMI テクノロジーを利用することにより、TZ シリーズファイア

メリット：

柔軟で統合されたセキュリティソリューション

- セキュア SD-WAN
- 強力な SonicOS オペレーティングシステム
- 高速 802.11ac ワイヤレス
- Power over Ethernet (PoE/PoE+)
- VLAN によるネットワークのセグメント化

優れた脅威防御とパフォーマンス

- 特許出願中の Real-Time Deep Memory Inspection テクノロジー
- 特許を取得した Reassembly-Free Deep Packet Inspection テクノロジー
- オンボックスおよびクラウドベースの脅威防御
- TLS/SSL の復号およびインスペクション
- 業界で認められたセキュリティの有効性
- 専門の Capture Labs 脅威研究チーム
- Capture Client によるエンドポイントセキュリティ

簡単な導入、セットアップ、および継続的な管理

- ゼロタッチ導入
- クラウドベースおよびオンプレミスの集中管理
- スケーラブルなファイアウォール製品
- 総所有コストの削減

ウォールはマルウェアやランサムウェアなどの脅威をゲートウェイでくい止めます。ファイアウォール境界外で使用されるモバイルデバイスの場合、SonicWall Capture Client は、機械学習やシステムロールバックなど高度な脅威防御手法を適用して、新しい層の保護を提供します。また、Capture Client は、信頼された TLS 証明書をインストールおよび管理することにより、TZ シリーズのファイアウォール上で暗号化された TLS トラフィックのディープインスペクション (DPI-SSL) も活用します。

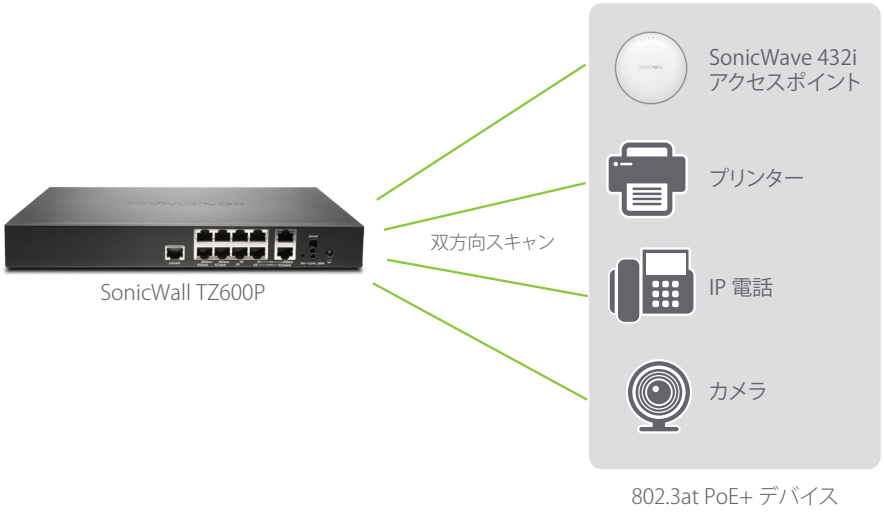
Web セッションを安全に保つための暗号化の使用は増加し続けており、暗号化されたトラフィックの脅威をスキャンする機能はファイアウォールにとって不可欠です。TZ シリーズのファイアウォールは、ポートやプロトコルに関係なく、TLS/SSL および SSH で暗号化された接続の、完全な復号とインスペクションを実行することによって、全面的な保護を実現します。ファイアウォールは、非準拠プロトコル、脅威、ゼロデイ、侵入、さらにはあらゆるパケット内を詳細に調べることにより、定義された基準も検索します。ディープパケットインスペクションエンジンは、暗号化を利用した見えない攻撃を検出して防御します。また、暗号化されたマルウェアのダウンロードをブロックし、感染の拡大を阻止して、コマンド & コントロール (C&C) 通信およびデータ漏出を防ぎます。包含および除外のルールにより、具体的な組織のコンプライアンス要件や法的要件に基づいて、復号とインスペクションの対象になるトラフィックを完全に制御してカスタマイズすることができます。

簡単な導入、セットアップ、および継続的な管理

SonicWall は、導入する場所に関係なく、TZ シリーズのファイアウォールおよび SonicWave 802.11ac Wave 2 アクセスポイントを容易に構成し管理できるようにしています。集中管理、レポート作成、ライセンシングおよび分析は、弊社のクラウドベースの Capture Security Center によって処理されます。これにより、SonicWall のセキュリティエコシステム全体を一元的に集中管理するために必要な最良の可視性、俊敏性、容量が提供されます。

Capture Security Center の極めて重要なコンポーネントは、ゼロタッチ導入です。このクラウドベース機能は、リモートおよびブランチオフィスのロケーションにおける SonicWall ファイアウォールの導入とプロビジョニングを簡素化し、迅速化します。このプロセスでは、人的介入は最小限に抑えられ、わずか数ステップで大規模なファイアウォールを完全に自動的に運用できます。これによって、インストールと構成に要する時間、コスト、複雑さが大きく削減されるとともに、セキュリティと接続性を即時かつ自動的にもたらすことができます。導入とセットアップが簡素化されると同時に、管理が容易であるという利点も兼ね備えているため、組織では総所有コストを削減して、高い投資収益率を実現することができます。

* 802.11ac は現在、SOHO/SOHO 250 モデルでは利用できません。SOHO/SOHO 250 モデルでは 802.11a/b/g/n をサポートしています。



お客様の PoE 対応デバイス向けの統合されたセキュリティと給電

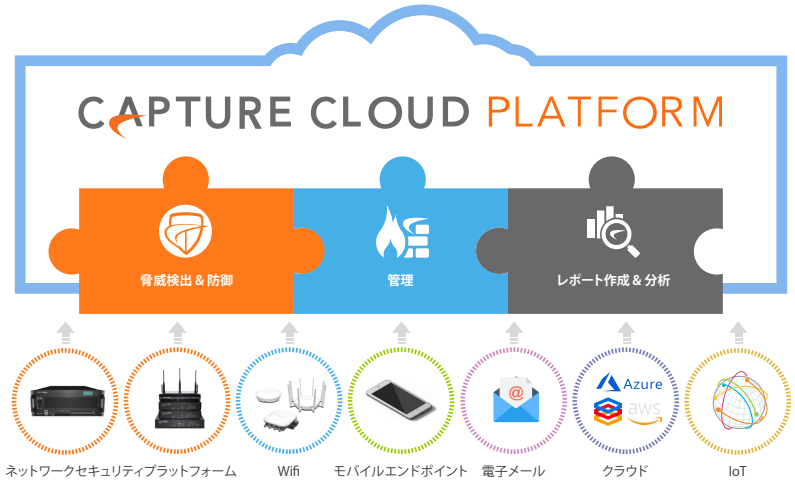
Power over Ethernet スイッチまたはインジェクタほどコストがかからず、複雑でもない方法で、お客様の PoE 対応デバイスに給電します。TZ300P および TZ600P ファイアウォールは、IEEE 802.3at テクノロジーを統合して、ワイヤレスアクセスポイント、カメラ、IP 電話、その他の PoE および PoE+ デバイスに給電します。このファイアウォールは、ディープパケットインスペクションというテクノロジーを使用して、各デバイスを出入りするすべてのトラフィックをスキャンし、暗号化された接続を経由していたとしても、マルウェアや侵入などの有害な脅威を除去します。

Capture Cloud Platform

SonicWall Capture Cloud Platform は、クラウドベースの脅威防御とネットワーク管理のほか、レポートと分析の機能をあらゆる規模の組織に提供します。このプラットフォームは、さまざまなソースから収集した脅威インテリジェンスを統合します。たとえば、賞を獲得したマルチエンジンのネットワークサンドボックスサービスである Capture Advanced Threat Protection や、世界中に配置された 100 万個を超える SonicWall のセンサーなどからデータを収集します。

ネットワークに入ってくるデータで未知の不正なコードが検出されると、SonicWall の社内に設置された専任の Capture Labs 脅威研究チームがシグネチャを開発します。このシグネチャは Capture Cloud Platform のデータベースに格納され、最新の保護を実現するためにお客様のファイアウォールに導入されます。新たな更新内容は即時に有効になり、リブートや中断は不要です。アプライアンスで用意されているシグネチャは、幅広い種類の攻撃を防御し、何万もの異なる脅威に対応します。TZ ファイアウォールは、アプライアンス上の対抗策に加えて、Capture Cloud Platform データベースに継続的にアクセスすることもできます。このデータベースにより、オンボードのシグネチャインテリジェンスは数千万のシグネチャで拡張されます。

Capture Cloud Platform は、脅威防御に加えて一元的な管理を実現します。管理者は、ネットワークアクティビティに関するリアルタイムレポートと履歴レポートを容易に作成できます。

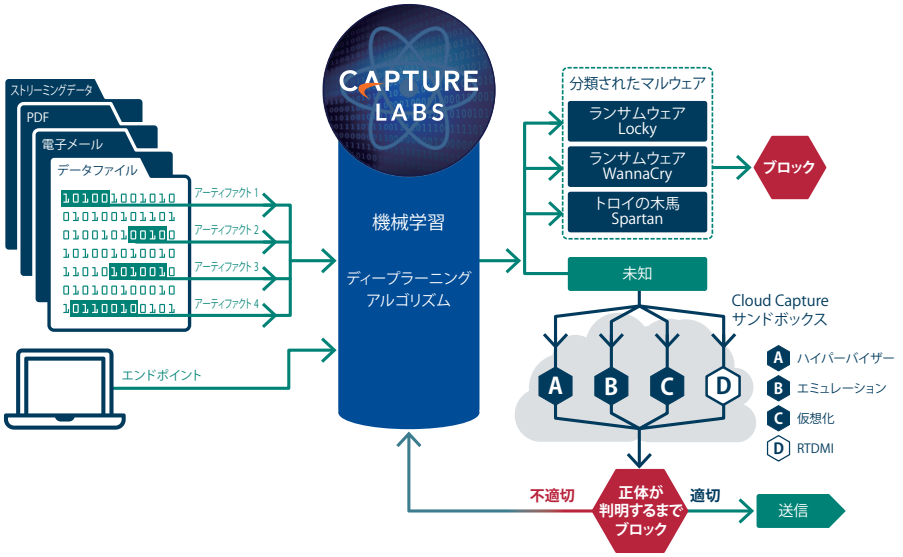


高度な脅威防御

自動化されたリアルタイムの侵入防止の中核を担うのが SonicWall Capture Advanced Threat Protection サービスです。このセキュリティサービスは、クラウドベースのマルチエンジンサンドボックスであり、ファイアウォールの脅威防御を拡張してゼロデイ脅威を検出、防止します。疑わしいファイルはクラウドに送信され、ディープラーニングアルゴリズムを使用して分析され、判定が下るまでゲートウェイで保持することもできます。Real-Time Deep Memory Inspection、仮想サンドボックス機能、フルシステムエミュレーション、ハイパーバイザーレベルの分析テクノロジー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。悪意のあるファイルであることが確認されると、そのファイルはブロックされ、Capture ATP 内でハッシュが即座に作成されます。この直後、以降の攻撃を防ぐためにシグネチャがファイアウォールに送られます。

サービスは、幅広いオペレーティングシステムと、実行可能プログラム、DLL、PDF、MS Office ドキュメント、アーカイブ、JAR、APK などの、さまざまな種類のファイルを分析します。

SonicWall Capture Client では、エンドポイントを全面的に保護するために、次世代のアンチウイルス技術と SonicWall のクラウドベースのマルチエンジンサンドボックスが統合されています。

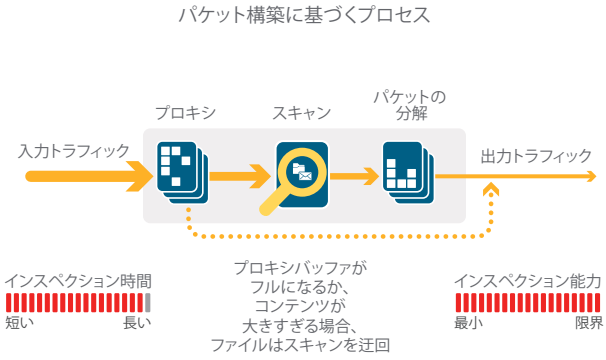


Reassembly-Free Deep Packet Inspection エンジン

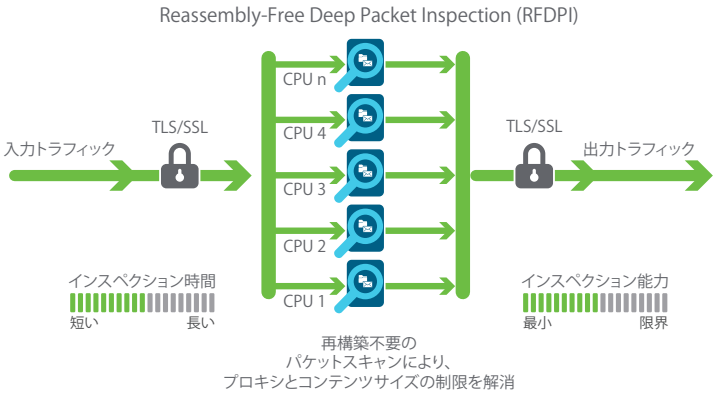
SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) は、プロキシやバッファを必要とせずにストリームベースの双方向トラフィック分析を高速で実行するシングルパス、低レイテンシのインスペクションシステムであり、侵入の試みやマルウェアのダウンロードを効率的に発見すると同時に、ポートやプロトコルにかかわらずアプリケーションのトラフィックを特定します。この独自のエンジンは、レイヤ 3 ～ 7 で脅威を検出するストリーミングトラフィックペイロードのインスペクションに基づいて動作し、検出エンジンを混乱させて悪意のあるコードをネットワークに忍び込ませることを狙った高度な回避方法を無効化するために、ネットワークストリームに対して大規模な正規化と復号を繰り返し実行します。

パケットは、TLS/SSL 復号などの必要な前処理が行われた後、3 つのシグネチャデータベース (侵入攻撃、マルウェア、およびアプリケーション) の単一かつ独自のメモリ表現と照らし合わせて分析されます。これにより、接続の状態はそれらの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、あらかじめ設定されたアクションが実行されます。

ほとんどの場合、接続は切断され適切なログと通知イベントが生成されます。一方で、インスペクション専用にエンジンを構成することもできます。また、アプリケーションを検出する場合は、アプリケーションが識別されると同時に、それ以降のアプリケーションストリームに対してレイヤ 7 帯域幅管理サービスが提供されるようにすることもできます。



競合するプロキシベースのアーキテクチャ



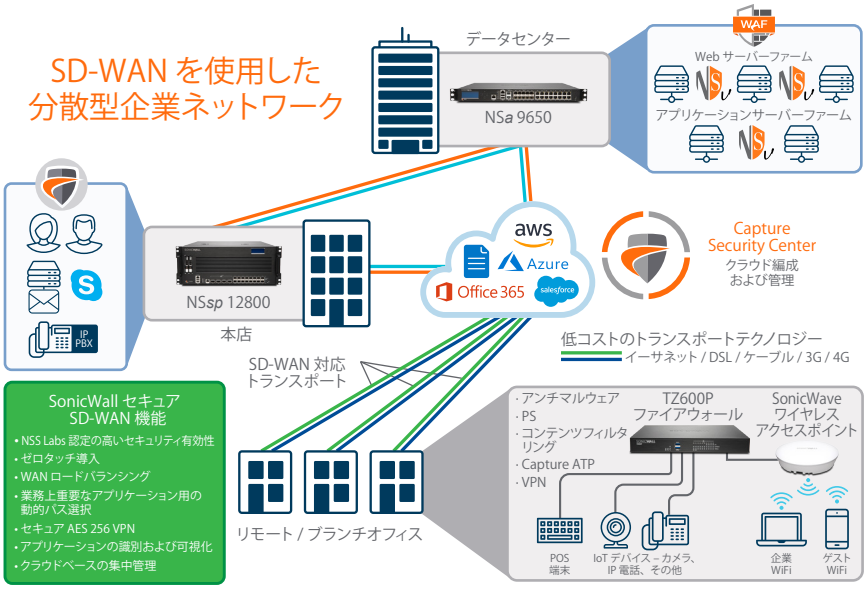
SonicWall のストリームベースのアーキテクチャ

集中化された管理とレポート作成

綿密に調整されたセキュリティガバナンス、コンプライアンス、リスク管理戦略を実施する必要がある、厳しい規制下にある組織のために、SonicWall は、相関性のある監査可能なワークストリームプロセスによって SonicWall ファイアウォール、ワイヤレスアクセスポイント、Dell N-Series および X-Series スイッチを管理する、統合された、セキュアで拡張可能なプラットフォームを管理者に提供します。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、管理とトラブルシューティングの複雑さを軽減して、セキュリティインフラストラクチャの運用をあらゆる面で管理することができます。たとえば、中央でのポリシーの管理と適用、リアルタイムでのイベント監視、ユーザーアクティビティ、アプリケーションの識別、フロー分析とフォレンジックス、コンプライアンスおよび監査用のレポート作成などの機能を備えています。さらに、企業はファイアウォールの変更管理要件をワークフローの自動化で満たします。この自動化により、適切なファイアウォールポリシーを適切なときに俊敏かつ確実に導入して、コンプライアンス規制に準拠することができます。オンプレミスでは SonicWall Global Management System、クラウドでは Capture Security Center をそれぞれ利用できる SonicWall の管理 / レポートソリューションは、ビジネスプロセスやサービスレベルごとにネットワークセキュリティを管理する一貫した手法を備えているので、デバイス単位の管理に比べて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。

分散ネットワーク

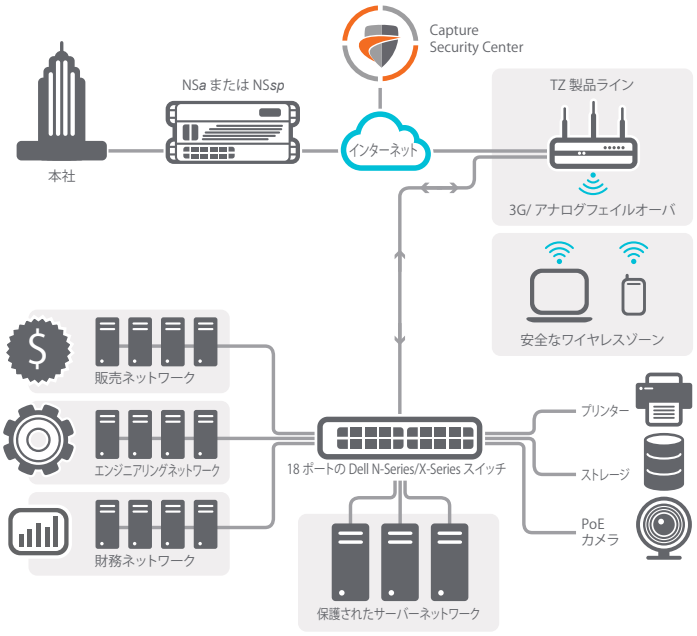
TZ シリーズファイアウォールは、その柔軟性から、分散型企業と単一サイト導入の両方に最適です。小売企業で使用されているような分散ネットワークでは、各サイトに独自の TZ ファイアウォールがあり、多くの場合 DSL、ケーブル、または 3G/4G 接続を使用してローカルプロバイダによってインターネットに接続しています。インターネットアクセスだけでなく、各ファイアウォールは、イーサネット接続を使用して、リモートサイトと中央の本店との間でパケットをやり取りしています。Web サービスおよび Office 365、Salesforce、その他の SaaS アプリケーションは、データセンターからサービスを提供されています。メッシュ VPN テクノロジーによって、IT 管理者は、すべてのロケーション間で安全にデータをやり取りできるように、ハブアンドスポーク構成を作成できます。



SonicOS の SD-WAN テクノロジーは、リモートおよびブランチサイトに導入された TZ ファイアウォールに完全に適しています。MPLS および T1 などの、より高価なレガシーテクノロジーに頼ることなく、SD-WAN を使用する組織では、より低コストのパブリックインターネットサービスを選択しながら、ハイレベルなアプリケーションの可用性と予測どおりのパフォーマンスを継続して達成できます。

Capture Security Center

SonicWall のクラウドベース Capture Security Center (CSC) は、分散ネットワークを束ねて、TZ ファイアウォールの導入、継続管理、リアルタイム分析の一元化を図ります。CSC の極めて重要な機能は、ゼロタッチ導入です。ファイアウォールを構成して複数のサイトに導入するのは時間がかかり、オンサイトの人員が必要になります。しかし、ゼロタッチ導入では、これらの問題を排除し、クラウドによって、リモートで SonicWall ファイアウォールの導入とプロビジョニングを簡素化および迅速化しています。同様に、CSC では、ネットワーク上の SonicWall デバイスをクラウドベースで一元管理できるので、継続的な管理が容易です。ネットワークセキュリティ環境の状況を完全に把握するために、SonicWall Analytics では、一元化されたビューで、ネットワーク内で発生しているすべての活動を確認することができます。組織は、アプリケーションの使用状況とパフォーマンスをより詳しく把握することができ、シャドー IT の危険性を軽減できます。



単一サイト

複数の単一サイトの導入の場合、統合されたネットワークセキュリティソリューションを持つことは、極めて利点が多くなります。TZ シリーズファイアウォールは、セキュリティの有効性が高く、内蔵 802.11ac ワイヤレスなどのオプションも使用できます (TZ300P および TZ600P の場合、PoE/PoE+ もサポート)。弊社ミッドレンジの NSa シリーズおよびハイエンドの NSsp シリーズと同じセキュリティエンジンが、TZ シリーズファイアウォールでは、SonicOS の広範な機能とともに搭載されています。構成および管理は、直観的な SonicOS UI を使用して容易に行えます。卓上型の小型形状なので、貴重なラックスペースを節減できます。

SonicWall TZ600 シリーズ（TZ600P は日本未提供）

セキュリティ、パフォーマンス、802.3at PoE+ サポートなどのオプションを安価で求めている新興企業や小売店、ブランチオフィスのために、SonicWall TZ600 は、エンタープライズクラスの各種機能と妥協の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	1.9 Gbps
脅威防御のスループット	800 Mbps
アンチマルウェアのスループット	800 Mbps
IPS スループット	1.2 Gbps
最大接続数	150,000
新規接続数 / 秒	12,000

TZ600P

PoE/PoE+ ポート (4 PoE/PoE+)

電源 LED　テスト LED　USB ポート (3G/4G WAN フェイルオーバ)　リンク / アクティビティ インジケータ LED

拡張モジュール　コンソール ポート　8x1 GbE スイッチ (構成可能)　X0 LAN ポート X1 WAN ポート　12V DC 2A 電源

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、極めて効果的で妥協の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
脅威防御のスループット	700 Mbps
アンチマルウェアのスループット	700 Mbps
IPS スループット	1.0 Gbps
最大接続数	150,000
新規接続数 / 秒	8,000

電源 LED　テスト LED　USB ポート (3G/4G WAN フェイルオーバ)　リンク / アクティビティ インジケータ LED

オプションの 802.11ac ワイヤレス

コンソール ポート　6x1 GbE スイッチ (構成可能)　X0 LAN ポート X1 WAN ポート　12V DC 2A 電源

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。ファイアウォールに内蔵されたオプションの 802.11ac デュアルバンドワイヤレスにより、柔軟なワイヤレス環境を導入できます。

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
脅威防御のスループット	600 Mbps
アンチマルウェアのスループット	600 Mbps
IPS スループット	900 Mbps
最大接続数	150,000
新規接続数 / 秒	6,000

電源 LED　テスト LED　USB ポート (3G/4G WAN フェイルオーバ)　リンク / アクティビティ インジケータ LED

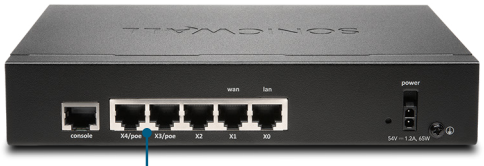
オプションの 802.11ac ワイヤレス

コンソール ポート　5x1 GbE スイッチ (構成可能)　X0 LAN ポート X1 WAN ポート　12V DC 2A 電源

SonicWall TZ350/TZ300 シリーズ（TZ300P は日本未提供）

SonicWall TZ300 および TZ350 シリーズは、ネットワークを高度な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、これらの UTM ファイアウォールでは、高速な侵入防止、アンチマルウェア、コンテンツ /URL フィルタリングが組み合わされており、さらにはノート PC、スマートフォン、タブレット向けの様々なセキュアなモバイルアクセスサポートと、オプションの内蔵 802.11ac ワイヤレスも利用できます。加えて、TZ300 ではオプションで 802.3at PoE+ がサポートされており、PoE 対応デバイスに電力を供給できます。

仕様	TZ350 シリーズ	TZ300 シリーズ
ファイアウォールのスループット	1.0 Gbps	750 Mbps
脅威防御のスループット	335 Mbps	235 Mbps
アンチマルウェアのスループット	335 Mbps	235 Mbps
IPS スループット	400 Mbps	300 Mbps
最大接続数	100,000	100,000
新規接続数 / 秒	6,000	5,000



TZ300P　PoE/PoE+ ポート (2 PoE または 1 PoE+)

電源 LED　テスト LED　USB ポート (3G/4G WAN フェイルオーバ)　リンク / アクティビティ インジケータ LED

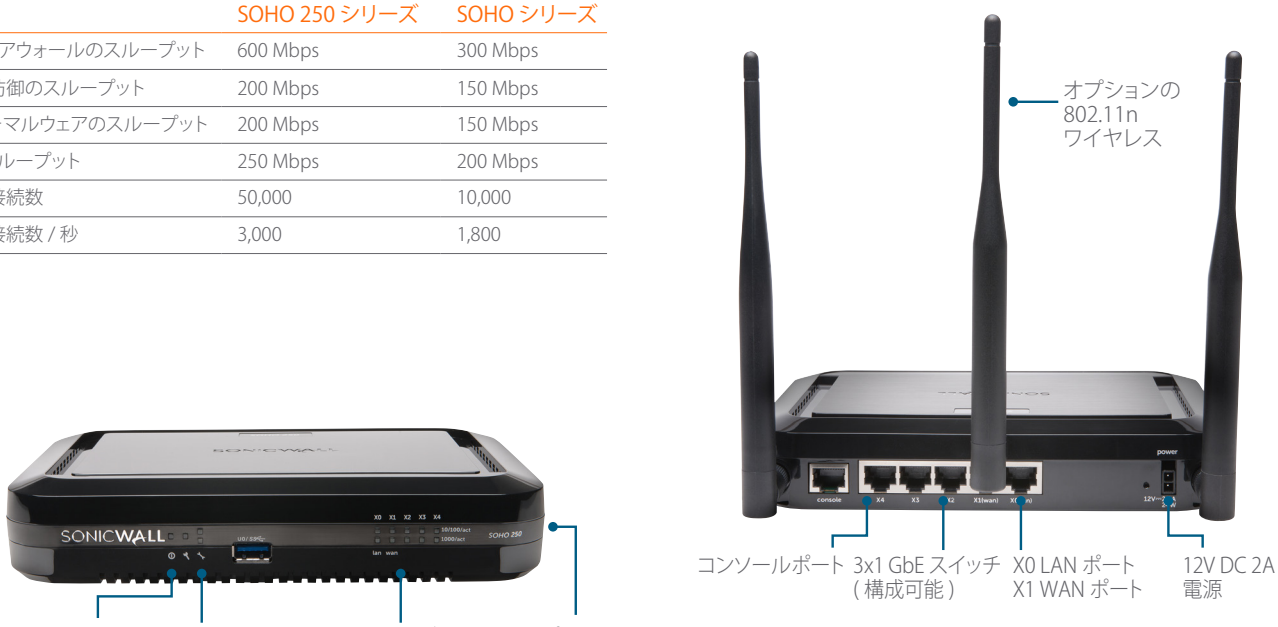
オプションの 802.11ac ワイヤレス

コンソール ポート　3x1 GbE スイッチ (構成可能)　X0 LAN ポート X1 WAN ポート　12V DC 2A 電源

SonicWall SOHO 250/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 250 および 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。オプションで 802.11n ワイヤレス機能を追加して、従業員、顧客、ゲストに安全なワイヤレス接続を提供できます。

仕様	SOHO 250 シリーズ	SOHO シリーズ
ファイアウォールのスループット	600 Mbps	300 Mbps
脅威防御のスループット	200 Mbps	150 Mbps
アンチマルウェアのスループット	200 Mbps	150 Mbps
IPS スループット	250 Mbps	200 Mbps
最大接続数	50,000	10,000
新規接続数 / 秒	3,000	1,800



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。SonicWall Advanced 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。

機能

RFDPI エンジン	
機能	説明
Reassembly-Free Deep Packet Inspection (RFDPI)	この特許を取得した独自のハイパフォーマンスインスペクションエンジンは、プロキシやバッファを必要とせずにストリームベースの双方向トラフィック分析を実行して、侵入の試みやマルウェアを発見し、ポートにかかわらずアプリケーショントラフィックを特定します。
双方向インスペクション	インバウンドとアウトバウンドの両方のトラフィックで同時に脅威をスキャンして、ネットワークがマルウェアの配布に使用されておらず、感染したマシンが内部に持ち込まれた場合に攻撃の踏み台にもならないことを確認します。
ストリームベースのインスペクション	プロキシとバッファを必要としないインスペクションテクノロジーにより、ファイルとストリームサイズに制限を設けることなく数百万の同時ネットワークストリームの DPI を極めて低いレイテンシで実行でき、一般的なプロトコルにも生の TCP ストリームにも適用できます。
高い並列性とスケーラビリティ	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動して、高い DPI スループットと極めて高速での新規セッション確立を実現し、要求の厳しいネットワークでのトラフィックの急増に対処します。
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。
ファイアウォールとネットワーキング	
機能	説明
セキュア SD-WAN	MPLS などのより高価なテクノロジーに取って代わるものであり、分散型企業の組織ではセキュア SD-WAN により、セキュアでハイパフォーマンスなネットワークをリモートサイト横断で構築、運用、管理し、常時利用可能な低コストのパブリックインターネットを使用して、データ、アプリケーション、サービスの共有を図ることができます。
REST API	ファイアウォールが、自社製、OEM 製、サードパーティ製のあらゆるインテリジェンスフィードを取り込んで活用し、ゼロデイ、悪意のある内部関係者、資格情報の漏洩、ランサムウェア、持続的標的型脅威などの、高度な脅威に対抗します。
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。
高可用性 / クラスタリング	SonicWall TZ500 および TZ600 モデルは、状態同期によるアクティブ / スタンバイを使用した高可用性をサポートしています。SonicWall TZ300 および TZ400 モデルは、アクティブ / スタンバイ同期を使用しない高可用性をサポートしています。SonicWall SOHO モデルには、高可用性機能は備わっていません。
DDoS/DoS 攻撃からの保護	SYN フラッド保護は、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 フラッド保護と接続速度の制限を使用して DoS/DDoS から保護します。
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 からの移行における初期段階にあります。SonicOS により、ハードウェアでフィルタリングとワイヤモードの実装がサポートされるようになります。
柔軟な導入オプション	TZ シリーズは、従来型の NAT、レイヤ 2 ブリッジ、ワイヤ、およびネットワークタップの各モードで導入できます。
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各方式を使用して、複数の WAN インターフェイス間で負荷を分散します。
高度なサービス品質 (QoS)	802.1p、DSCP 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って、重要な通信を保証します。
H.323 ゲートキーパーおよび SIP プロキシのサポート	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。
単体およびカスケード接続された Dell N-Series および X-Series スイッチの管理	Dell の N-Series および X-Series ネットワークスイッチの追加ポートのセキュリティ設定 (Portshield、HA、PoE、PoE+ など) を、ファイアウォール管理ダッシュボードを使用して一元的に管理します (SOHO モデルでは使用不可)。
生体認証	簡単には複製または共有できない指紋認識などのモバイルデバイス認証をサポートし、ネットワークアクセス用のユーザー ID をセキュアに認証します。
オープン認証とソーシャルログイン	ゲストユーザーが、パススルー認証を使用して、ホストのワイヤレスゾーン、LAN ゾーン、または DMZ ゾーン経由で、Facebook、Twitter、Google+ などのソーシャルネットワーキングサービスの資格情報でインターネットやその他のゲストサービスにサインインし、アクセスすることができます。
ワイヤレスネットワークのセキュリティ	SonicWall TZ300 から TZ500 で内蔵オプションとして使用可能な 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を発揮し、より広い通信範囲と高い信頼性を実現しました。SonicWall SOHO モデルでは、オプションの 802.11 a/b/g/n が利用可能です。
管理とレポート作成	
機能	説明
クラウドベースおよびオンプレミスの管理	SonicWall アプライアンスの構成および管理は、SonicWall Capture Security Center を使用してクラウド経由で、および SonicWall Global Management System (GMS) を使用してオンプレミスで行うことができます。
強力な単一デバイス管理	包括的なコマンドラインインターフェイスを備え、SNMPv2/3 をサポートしているほか、直観的な Web ベースのインターフェイスによる迅速かつ容易な構成が可能です。
IPFIX/NetFlow アプリケーションフローレポート	アプリケーションのトラフィックの分析データと使用状況のデータを IPFIX または NetFlow プロトコルを通じてエクスポートして、リアルタイムでの、および過去に遡っての監視とレポートを行います。そのために、拡張機能を備えた、IPFIX および NetFlow をサポートするツールを使用できます。

仮想プライベートネットワーキング	
機能	説明
VPN の自動プロビジョニング	SonicWall ファイアウォール間における初期のサイト間 VPN ゲートウェイのプロビジョニングを自動化することにより、複雑な分散ファイアウォールの導入が簡素化され、わずかな作業で済むようになるとともに、セキュリティと接続性が瞬時に、そして自動的に確保されます。
サイト間 IPSec VPN	ハイパフォーマンスな IPSec VPN により、TZ 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 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、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 を使用する場合に、プライマリ VPN とセカンダリ VPN を、すべての VPN セッションのシームレスな自動フェイルオーバーとフェイルバックが可能になるよう構成できます。
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/Citrix1/Terminal Services1 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 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。国やボットネットのカスタムリストを作成して、IP アドレスに誤って関連付けられている国やボットネットのタグを無効にすることができます。誤分類による IP アドレスの不要なフィルタリングを防止します。
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。国やボットネットのカスタムリストを作成して、IP アドレスに誤って関連付けられている国やボットネットのタグを無効にすることができます。
CAPTURE ADVANCED THREAT PROTECTION	
機能	説明
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ー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。
Real-Time Deep Memory Inspection (RTDMI)	この特許出願中のクラウドベースの技術は、表立って悪意のある動作を実行せずにカスタム暗号化で武器を隠しているマルウェアを検出し、ブロックします。RTDMI エンジンは、メモリ内で武器を示すようにマルウェアに強制することで、大量に出回っているゼロデイ脅威と未知のマルウェアをプロアクティブに検出し、ブロックします。
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。
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、個別にまたはグループとして分析します。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展開	ファイルが不正であると特定されると、SonicWall Capture ATP 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配布され、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のほか、URL、IP、ドメインのレピュテーションデータベースにもシグネチャが 48 時間以内に送られます。
Capture Client	Capture Client は、高度なマルウェア防御、暗号化トラフィックへの可視化サポートなど、複数のエンドポイント保護機能を提供する統合クライアントプラットフォームです。このプラットフォームでは、多層型の保護技術、包括的なレポート機能、エンドポイント保護を利用できます。
暗号化された脅威防御	
機能	説明
TLS/SSL の復号および インスペクション	TLS/SSL で暗号化されたトラフィックを復号して、マルウェア、侵入、データ漏洩がないかどうかを、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、コンテンツの制御ポリシーを適用して、暗号化されたトラフィックに潜む脅威を防御します。SOHO を除いたすべての TZ シリーズ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 では別途ライセンスとして販売されます。
SSH インスペクション	SSH のディープパケットインスペクション (DPI-SSH) により、SSH トンネルを通過するデータを復号して検査し、SSH を利用する攻撃を防ぎます。
侵入防止	
機能	説明
対抗策に基づく保護	緊密に統合された侵入防止システム (IPS) では、シグネチャや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 を超える攻撃分野をカバーする広範な IPS 対抗策のリストを随時更新しています。新たな更新は即座に適用され、再起動する必要も、サービスが中断されることもありません。
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散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。

侵入防止 (続き)	
機能	説明
ボットネットによるコマンドアンドコントロール (CnC) の検知およびブロック	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	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を悪用する最新の手口やテクニックに対抗できるように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 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
ゲートウェイでのアンチマルウェア	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、その他のマルウェアがファイルに潜んでないかどうかを調べます。ファイルの長さやサイズに制限はなく、すべてのポートと TCP ストリームがスキャンの対象となります。
Capture Cloud のマルウェア対策	SonicWall のクラウドサーバーには数千万件におよぶ脅威のシグネチャのデータベースがあり、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により、オンボードのシグネチャデータベースの機能を補強して、RFDPI で扱う脅威の範囲を広げることができます。
24 時間体制のセキュリティ更新	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。
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のみを重点的に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。
アプリケーションインテリジェンスおよび制御	
機能	説明
アプリケーションの制御	RFDPI エンジンが識別するアプリケーションやアプリケーションの諸機能を、数千におよぶアプリケーションシグネチャが格納され、継続的に拡張されているデータベースと照合することにより制御し、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。
詳細な制御	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 / 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およびコンテンツフィルタリングクライアントを利用して、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 HTTP/HTTPS Web サイトへのアクセスをブロックします。
エンフォースドコンテンツフィルタリングクライアント	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 Windows、Mac OS、Android、Chrome の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。
詳細な制御	事前定義されているカテゴリまたはカテゴリの任意の組み合わせを使用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。
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。
エンフォースドアンチウイルス / アンチスパイウェア	
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に適切なアンチウイルスソフトウェアや DPI-SSL 証明書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管理で通常発生する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のオプション	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。
次世代アンチウイルス	Capture Client は、人工知能 (AI) エンジンを使用して実行可能になる前に脅威を判定し、以前の感染前の状態にロールバックします。
スパイウェア対策	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。

SonicOS の機能の概要

ファイアウォール
- ステートフルパケットインスペクション
- Reassembly-Free Deep Packet Inspection
- DDoS 攻撃の防御 (UDP/ICMP/SYN フラッド)
- IPv4/IPv6 のサポート
- リモートアクセスのための生体認証
- DNS プロキシ
- REST API

SSL/SSH の復号およびインスペクション [1]
- TLS/SSL/SSH に対応した ディープパケットインスペクション
- オブジェクト、グループ、 またはホスト名の包含 / 除外
- TLS/SSL 制御
- ゾーンまたはルールごとの 詳細な DPI SSL 制御

Capture Advanced Threat Protection [1,2]
- Real-Time Deep Memory Inspection
- 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
- ハイパーバイザーレベルの分析
- 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の調査
- 自動および手動の送信
- リアルタイムの 脅威インテリジェンスの更新
- 正体が判明するまでブロック
- Capture Client

侵入防止 [1]
- 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
- 詳細な IPS ルール機能
- GeoIP/ ボットネットのフィルタリング [2]
- 正規表現マッチング

アンチマルウェア [1]
- 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

アプリケーションの識別 [1]
- アプリケーションの制御
- アプリケーションの帯域幅管理
- カスタムの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
- 包括的なアプリケーションシグネチャの データベース

トラフィックの可視化と分析
- ユーザーアクティビティ
- アプリケーション / 帯域幅 / 脅威の使用状況
- クラウドベースの分析

HTTP/HTTPS Web コンテンツフィルタリング [1]
- 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
- ポリシーベースフィルタリング (除外 / 包含)
- HTTP ヘッダーの挿入
- 帯域幅管理 CFS 評価カテゴリ
- アプリケーションの制御が可能な 統合ポリシーモデル
- コンテンツフィルタリングクライアント

VPN
- VPN の自動プロビジョニング
- サイト間接続のための 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
- iOS、Mac OS X、Windows、Chrome、 Android、Kindle Fire のモバイル接続
- ルートベース VPN (OSPF、RIP、BGP)

ネットワーク
- セキュア SD-WAN
- PortShield
- 強化されたログ機能
- レイヤ 2 の QoS
- ポートセキュリティ
- 動的ルーティング (RIP/OSPF/BGP)
- SonicWall 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 (ToS/ メトリックおよび ECMP)
- 非対称ルーティング
- DHCP サーバー
- NAT
- 帯域幅の管理
- 高可用性 - 状態同期による アクティブ / スタンバイ [3]
- インバウンド / アウトバウンドの ロードバランシング
- L2 ブリッジモード、NAT モード
- 3G/4G WAN フェイルオーバ
- Common Access Card (CAC) のサポート

VoIP
- 詳細な QoS 制御
- 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
- SonicWall GMS および Capture Security Center による 集中化された管理とレポート
- ログ
- Netflow/IPFix エクスポート
- クラウドベースの構成バックアップ
- アプリケーションと帯域幅の可視化
- IPv4 と IPv6 の管理
- カスケード接続のスイッチを含む Dell N-Series および X-Series スイッチ管理 [2]

内蔵ワイヤレス
- 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 [2]
- WIDS/WIPS
- 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

[1] サブスクリプションの追加が必要です
[2] SOHO/SOHO ワイヤレスでは利用不可
[3] 状態同期による高可用性は、SonicWall TZ500 モデルと SonicWall TZ600 モデルでのみ利用可能

SonicWall TZ シリーズのシステム仕様

ファイアウォール全般	SOHO シリーズ	SOHO 250 シリーズ	TZ300 シリーズ	TZ350 シリーズ
オペレーティングシステム	SonicOS			
インターフェイス	5x1GbE、1 USB、1 コンソール		5x1GbE、1 USB、1 コンソール	5x1GbE、1 USB、1 コンソール
Power over Ethernet (PoE) のサポート	—	—	TZ300P - 2 ポート (2 PoE または 1 PoE+)	—
拡張	USB			
管理	CLI、SSH、Web UI、Capture Security Center、GMS、REST API			
シングルサインオン (SSO) ユーザー	250	350	500	500
VLAN インターフェイス	25			
サポートされるアクセスポイント (最大)	2	4	8	8
ファイアウォール /VPN パフォーマンス	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 シリーズ**
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	600 Mbps	750 Mbps	1.0 Gbps
脅威防御のスループット [2]	150 Mbps	200 Mbps	235 Mbps	335 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]	—	275 Mbps	375 Mbps	600 Mbps
IPS のスループット [2]	200 Mbps	250 Mbps	300 Mbps	400 Mbps
アンチマルウェアインスペクションのスループット [2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
TLS/SSL インスペクションと復号スループット (DPI SSL)[2]	30 Mbps	50 Mbps	60 Mbps	65 Mbps
IPSec VPN のスループット [3]	150 Mbps	200 Mbps	300 Mbps	430 Mbps
接続数 / 秒	1,800	3,000	5,000	6,000
最大接続数 (SPI)	10,000	50,000	100,000	100,000
最大接続数 (DPI)	10,000	50,000	90,000	90,000
最大接続数 (DPI SSL)	250	25,000	25,000	25,000
VPN	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 シリーズ**
サイト間 VPN トンネル	10	10	10	15
IPSec VPN クライアント (最大)	1 (6)	1 (6)	2 (12)	2 (12)
SSL VPN ライセンス数 (最大)	1 (10)	1 (25)	1 (50)	1 (75)
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)
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、14v			
ルートベース VPN	RIP、OSPF、BGP			
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、Chrome、Windows 8.1 (Embedded)			
セキュリティサービス	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 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			
Comprehensive Anti-Spam Service	サポート対象			
アプリケーションの可視化	なし	あり	あり	あり
アプリケーションの制御	あり	あり	あり	あり
Capture による高度な脅威対策	なし	あり	あり	あり
ネットワーク	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 シリーズ**
IP アドレスの割り当て	静的、(DHCP PPPoE、L2TP、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			
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)			

SonicWall TZ シリーズの仕様 (続き)

ネットワーキング (続き)	SOHO シリーズ	SOHO 250 シリーズ	TZ300 シリーズ	TZ350 シリーズ
認証	LDAP (複数ドメイン)、XAUTH/RADIUS、SSO、Novell、内部ユーザーデータベース		LDAP (複数ドメイン)、XAUTH/RADIUS、SSO、Novell、内部ユーザーデータベース、Terminal Services、Citrix、Common Access Card (CAC)	
ローカルユーザーデータベース	150			
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			
認定規格	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 (ファイアウォールおよび IPS)			
Common Access Card (CAC)	サポート対象			
高可用性	なし		Active/Standby	
ハードウェア	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 シリーズ**
形状	デスクトップ			
電源	24 W (外付)		24 W (外付) 65 W (外付) (TZ300P のみ)	24 W (外付)
最大消費電力 (W)	6.4 / 11.3	6.9 / 11.3	6.9 / 12.0	6.9 / 12.0
入力電源	100 ～ 240 VAC、50 ～ 60 Hz、1 A			
総発熱量	21.8 / 38.7 BTU	23.5 / 38.7 BTU	23.5 / 40.9 BTU	23.5 / 40.9 BTU
寸法	3.6 x 14.1 x 19 cm (1.42 x 5.55 x 7.48 インチ)		3.5 x 13.4 x 19 cm (1.38 x 5.28 x 7.48 インチ)	3.5 x 13.4 x 19 cm (1.38 x 5.28 x 7.48 インチ)
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
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
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
MTBF (年)	58.9 / 56.1 (ワイヤレス)	56.1	56.1	56.1
環境 (動作 / 保管)	0 ～ 40℃ (32 ～ 105° F)/-40 ～ 70℃ (-40 ～ 158° F)			
湿度	5 ～ 95% (結露しないこと)			
規制	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 シリーズ**
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	
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	
内蔵ワイヤレス	**SOHO シリーズ**	**SOHO 250 シリーズ**	**TZ300 シリーズ**	**TZ350 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	

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	SOHO 250 シリーズ	TZ300 シリーズ	TZ350 シリーズ
動作チャネル	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地域に基づく			
送信電力制御	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	
変調技術スペクトラム	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)、802.11b: 直交周波数分割多重方式 (OFDM)	

* 将来用。

[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] 脅威防御 / ゲートウェイ AV/ 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。脅威防御のスループットは、ゲートウェイ AV、アンチスパイウェア、IPS およびアプリケーションの制御を有効にして測定しました。

[3] VPN のスループットは、RFC 2544 準拠のパケットサイズ (1280 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] すべての 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 のワイヤレスアクセスポイント製品をご利用ください。

SonicWall TZ シリーズのシステム仕様 (続き)

ファイアウォール全般	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	
インターフェイス	7x1GbE、1 USB、 1 コンソール	8x1GbE、2 USB、 1 コンソール	10x1GbE、2 USB、 1 コンソール、 1 拡張スロット
Power over Ethernet (PoE) のサポート	—	—	TZ600P - 4 ポート (4 PoE または 4 PoE+)
拡張	USB	2 USB	拡張スロット (背面)*、2 USB
管理	CLI、SSH、Web UI、Capture Security Center、GMS、REST API		
シングルサインオン (SSO) ユーザー	500	500	500
VLAN インターフェイス	50	50	50
サポートされるアクセスポイント (最大)	16	16	24
ファイアウォール /VPN パフォーマンス	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
ファイアウォールインスペクションの スループット [1]	1.3 Gbps	1.4 Gbps	1.9 Gbps
脅威防御のスループット [2]	600 Mbps	700 Mbps	800 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]	1.2 Gbps	1.3 Gbps	1.8 Gbps
IPS のスループット [2]	900 Mbps	1.0 Gbps	1.2 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]	600 Mbps	700 Mbps	800 Mbps
TLS/SSL インスペクションと 復号スループット (DPI SSL)[2]	180 Mbps	225 Mbps	300 Mbps
IPSec VPN のスループット [3]	900 Mbps	1.0 Gbps	1.1 Gbps
接続数 / 秒	6,000	8,000	12,000
最大接続数 (SPI)	150,000	150,000	150,000
最大接続数 (DPI)	125,000	125,000	125,000
最大接続数 (DPI SSL)	25,000	25,000	25,000
VPN	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
サイト間 VPN トンネル	20	25	50
IPSec VPN クライアント (最大)	2 (27)	2 (27)	2 (27)
SSL VPN ライセンス数 (最大)	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)
暗号化 / 認証	DES、3DES、AES (128、192、256 ビット)/MD5、SHA-1、Suite B 暗号方式		
キー交換	Diffie Hellman グループ 1、2、5、14v		
ルートベース VPN	RIP、OSPF、BGP		
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、Chrome、Windows 8.1 (Embedded)		
セキュリティサービス	**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		
Comprehensive Anti-Spam Service	サポート対象		
アプリケーションの可視化	あり	あり	あり
アプリケーションの制御	あり	あり	あり
Capture による高度な脅威対策	あり	あり	あり
ネットワーク	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
IP アドレスの割り当て	静的、(DHCP PPPoE、L2TP、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		
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)		

SonicWall TZ シリーズのシステム仕様 (続き)

ネットワーク	TZ400 シリーズ	TZ500 シリーズ	TZ600 シリーズ
認証	LDAP (複数ドメイン)、XAUTH/RADIUS、SSO、Novell、内部ユーザーデータベース、Terminal Services、Citrix、Common Access Card (CAC)		
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 (ファイアウォールおよび IPS)		
Common Access Card (CAC)	サポート対象		
高可用性	Active/Standby	ステートフル同期による Active/Standby	
ハードウェア	**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	
電源	24 W (外付)	36W (外付)	60 W (外付) 180 W (外付) (TZ600P のみ)
最大消費電力 (W)	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	31.3 / 47.1 BTU	45.9 / 60.5 BTU	55.1 BTU
寸法	3.5 x 13.4 x 19 cm (1.38 x 5.28 x 7.48 インチ)	3.5 x 15 x 22.5 cm (1.38 x 5.91 x 8.86 インチ)	3.5 x 18 x 28 cm (1.38 x 7.09 x 11.02 インチ)
重量	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	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	1.37 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)	54.0	40.8	18.4
環境 (動作 / 保管)	0 ～ 40℃ (32 ～ 105° F)/-40 ～ 70℃ (-40 ～ 158° F)		
湿度	5 ～ 95% (結露しないこと)		
規制	**TZ400 シリーズ**	**TZ500 シリーズ**	**TZ600 シリーズ**
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、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
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	—

SonicWall TZ シリーズのシステム仕様 (続き)

内蔵ワイヤレス	TZ400 シリーズ	TZ500 シリーズ	TZ600 シリーズ
標準	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、 802.11ac: 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、 802.11ac: 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		—
送信電力制御	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、 802.11ac: 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		—
変調技術スペクトラム	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)		—

法令遵守モデル番号

SOHO/SOHO ワイヤレス	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 ワイヤレス	APL41-0D6/APL41-0BA
TZ300/TZ300 ワイヤレス / TZ300P	APL28-0B4/APL28-0B5/ APL47-0D2
TZ350/TZ350 ワイヤレス	APL28-0B4/APL28-0B5
TZ400/TZ400 ワイヤレス	APL28-0B4/APL28-0B5
TZ500/TZ500 ワイヤレス	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3

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

Datasheet-TZ Series-US-VG-MKTG5541

SONICWALL®