Release Notes

SonicOS | SonicOS 5.8.1.7-5o+ リリースノート (TZ 105W/205W 装置)

目次

プラットフォームの互換性

SonicOS 5.8.1.7-5o+ リリースは、下記の SonicWALL 精密パケット検査 (DPI) セキュリティ装置をサポートします。

- SonicWALL TZ 105 Wireless
- SonicWALL TZ 205 Wireless

SonicWALL WAN 高速化装置シリーズ (WXA 500 Live CD、WXA 2000/4000 Appliances) は、5.8.1.7-5o+ で動作している NSA E-Class、NSA、および TZ 装置と共に使うことがサポートされています。WXA シリーズの推奨される最低限のファームウェア バージョンは 1.1.1 です。

ご使用の前に

最新版をご利用ください

SonicWALLセキュリティ装置を実運用環境に配備する前に、常に最新のファームウェアにアップグレードすることを推奨します。

最新のファームウェアとリリースノートは、https://www.mysonicwall.com から入手できます。
(https://www.mysonicwall.com の利用には、ユーザ登録が必要です。)

ファームウェアのアップロード手順については、本リリースノート後半の、「SonicOSイメージのアップグレード手順」セクションを参照してください。

ブラウザ サポート

可視化機能を持つ SonicOS は、最新のブラウザでサポートされる HTML 5 といった先進のブラウザ技術を使います。SonicWALL は SonicOS の管理に最新の Chrome、Firefox、Internet Explorer、または Safari ブラウザの使用を推奨します。

本リリースでは、下記のウェブ ブラウザをサポートしています。

- Chrome 11.0 以降 (ダッシュボードのリアルタイム グラフィック表示に対する推奨ブラウザ)
- Firefox 4.0 以降
- Internet Explorer 8.0 以降 (互換モードは使わないでください)
- Safari 5.0 以降

SonicWALL 装置のシステム管理には、モバイル機器のブラウザは推奨されません。

SonicOS 5.8.1.7 での拡張

SonicOS 5.8.1.7 からは、SonicOS のウェブ ベースの管理インターフェースへの HTTP アクセスが既定で無効です。SonicOS 5.8.1.7 が工場出荷時の設定を使って動作している場合、管理者は管理インターフェースに HTTPS を使って **https://192.168.168.168** からアクセスできます。

以前のファームウェア バージョンからアップグレードした場合、以前の設定で HTTP 管理が許可されていれば、アップグレード後も HTTP 管理は許可されたままです。

備考: SonicWALL GMS によって VPN トンネルを通してファイアウォールが管理されている場合は、HTTP 管理が有効になっている必要があります。これは GMS 管理トンネルまたは既存の VPN トンネルのどちらを使う場合でも適用されます。

「システム ＞ 管理」ページに、管理者が HTTP 管理を全体的に有効化/無効化することが可能な新設の「**HTTP を介しての管理を許可する**」チェックボックスがあります。

装置モデルによりサポートされる機能

以下の表は、SonicOS 5.8 の主な新機能の一覧で、どの装置モデルがそれらをサポートしているかを示します。

機能 / 拡張	TZ 105 Wireless	TZ 205 Wireless
無線クライアント ブリッジ サポート	サポート	サポート
アプリケーション フロー監視		

リアルタイム監視		
パケット監視の拡張	サポート	サポート
ログ > フロー報告		
アプリケーション制御詳細	サポート	サポート
アプリケーション ルール	サポート	サポート
DPI-SSL		
ステートレス高可用性		サポート
クラウド GAV	サポート	サポート
NTP 認証種別	サポート	サポート
リンク統合		
ポート冗長		
CFS 拡張	サポート	サポート
IPFIX と NetFlow レポート		
VLAN サブ インターフェース	サポート	サポート
SonicPoint VAP	サポート	サポート
CASS 2.0	サポート	サポート
接続制限の拡張	サポート	サポート
動的 WAN スケジュール	サポート	サポート
ブラウザ NTLM 認証	サポート	サポート
LDAP からのユーザ インポート	サポート	サポート
SSL VPN NetExtender クライアント更新	サポート	サポート
DHCP スケーラビリティの拡張	サポート	サポート
SIP アプリケーション層の拡張	サポート	サポート
複数 VPN クライアント プロポーザルの受諾	サポート	サポート
WAN 高速化サポート	サポート	サポート

アプリケーション フロー監視からのアプリケーション制御ポリシー設定		
グローバル帯域幅管理による使用感の拡張	サポート	サポート
アプリケーション使用および危険性報告		
地域 IP フィルタと Botnet コマンドおよびコントロール フィルタ		
ワイヤとタップ モード		
ユーザ定義可能なログイン ページ	サポート	サポート
アップグレード後のアンチウィルス除外の維持	サポート	サポート
ネットワーク インターフェースに対する管理トラフィックのみのオプション	サポート	サポート
TSR に対する現在のユーザおよびユーザ詳細のオプション	サポート	サポート
ユーザ監視ツール		
ユーザ認証をバイパスさせる URL の自動設定	サポート	サポート

SonicOS 5.8 注目の機能

以下は、SonicOS 5.8 で提供された注目の機能です。

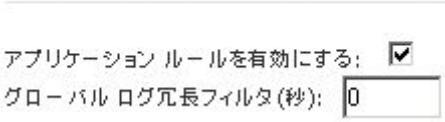
- **アプリケーション インテリジェンス + 制御** - この機能は、更なるネットワーク セキュリティのための 2 つの要素を持ちます。

(a) **識別**: リアルタイムでアプリケーションを識別して、ユーザのネットワーク動作を追跡します。
(b) **制御**: 帯域幅制限ポリシーに基づいて、アプリケーションとユーザのトラフィックを、許可／拒否します。
管理者は以下に基づいて、ネットワーク トラフィック フローをフィルタするネットワーク ポリシー オブジェクト ベースの制御ルールを容易に作成できます。

- 危険であることが知られていて執行が難しい、**アプリケーション** のシグネチャー一致による遮断
- 信頼された **ユーザとユーザ グループ** および、ゲスト サービスのリアルタイム ネットワーク アクティビティ参照
- **内容評価済み種別** との一致

ネットワーク セキュリティ管理者は、これで、ネットワークを通るトラフィック フロー内で、アプリケーション レベル、ユーザ レベル、そして内容レベルのリアルタイム視野を手に入れました。 管理者は、即時にネットワークのトラフィック再現手配の措置を講じて、素早くウェブ使用の悪用を識別して、組織をマルウェアの侵入から保護できます。 管理者は帯域幅を多く取るウェブサイトとアプリケーションへのアクセスを制限して、重要なアプリケーションとサービスに高い優先度を確保して、取り扱いに慎重を要するデータが SonicWALL で保護されたネットワークから逃れることを防ぎます。
SonicOS 5.8 で動作する新しい装置は、登録時に自動的にアプリケーション制御の 30 日間の無料トライアルを受け取ります。
SonicOS 5.8 にアップグレードする、**かつ**、すでに GAV/IPS/AS、トータル セキュア、または、包括的ゲートウェイ セキュリティ スイート (CGSS) がライセンスされている SonicWALL 装置は、自動的にアプリケーション制御ポリシー作成のために必要なアプリケーション制御の無料ライセンスを受け取ります。
アプリケーション制御機能の利用を開始するには、「ファイアウォール > アプリケーション制御詳細」ページで、「アプリケーション制御を有効にする」オプションを選択します。

アプリケーション ルール（アプリケーション制御ライセンスに含まれる）を使ったポリシーを作成するには、「ファイアウォール > アプリケーション ルール」ページの「アプリケーション ルールを有効にする」を選択します。



- **グローバル帯域幅管理** - グローバル帯域幅管理は、帯域幅管理 (BWM) 設定の使い勝手を改良して、WAN だけではなく、すべてのインターフェース上の受信および送信トラフィックに対して管理されたパケットのスループット能力を向上させます。 新設の「ファイアウォール設定 ＞ 帯域幅管理」ページにより、ネットワーク管理者は最小保証帯域と最大帯域の指定、およびトラフィックに対する異なる優先レベル順の制御が可能です。これらのグローバル設定は、ファイアウォール アクセス ルールおよびアプリケーション制御ポリシーで使用されます。グローバル帯域幅管理は、以下を提供します。
- すべてのインターフェース上での容易な帯域幅管理
- 受信および送信トラフィック両方の帯域幅管理

- ファイアウォール ルールおよびアプリケーション制御ルール毎の帯域幅管理の優先順位指定サポート
- すべてのトラフィックに対する既定の帯域幅管理キュー
- 「ダッシュボード ＞ アプリケーション フロー監視」ページからの帯域幅管理の直接適用サポート

グローバル帯域幅管理は、各物理インターフェースに適用可能な 8 つの優先順位キューを提供します。
以下は、新設された「**ファイアウォール設定 ＞ 帯域幅管理**」ページです。

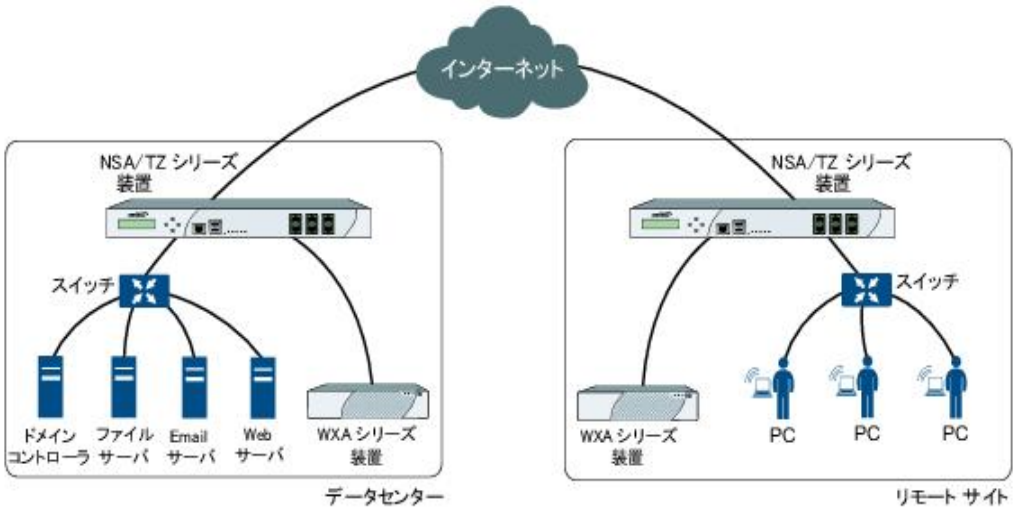
「**帯域幅管理種別**」として、「**WAN**」または「**グローバル**」のどちらかを選択できます。

備考: 帯域幅管理のモードを切り替えると、ファイアウォール アクセス ルール内の帯域幅管理設定は既定に戻り、すべての個別設定の再構成が必要になります。アプリケーション制御ポリシー内の既定の BWM 動作は、既定の優先レベルを用いて自動的に WAN BWM または、グローバル BWM に変換されます。

グローバル優先順位キュー テーブル内で、各「**優先順位**」キューに対して「**保証**」および「**最大/バースト**」速度を設定できます。この速度は、パーセンテージで指定します。実際の速度は、BWM がインターフェースに適用される際に動的に決定されます。インターフェースに設定された帯域幅は、最終的な値の計算に使われます。すべての保証帯域の合計は、100% を超えられず、保証帯域は、キュー毎の最大帯域幅より大きくできません。

- **帯域幅管理監視ページ** - 新しい帯域幅管理監視ページには、送信および受信ネットワークトラフィックに対するインターフェース毎の帯域幅管理が表示されます。帯域幅管理監視グラフはリアルタイム、最高、高、中高、中、中低、低、最低のポリシー設定に対して利用可能です。表示範囲は 60 秒、2 分、5 分、10 分 (既定) に設定可能です。更新間隔は 3 から 30 秒の間で設定可能です。帯域幅管理の優先度は保証、最大、破棄で表示されます。

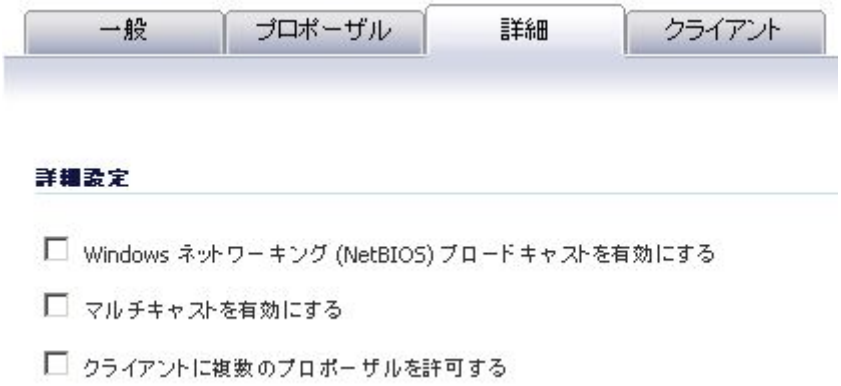
- **WAN 高速化** - SonicOS 5.8.1.7 は、SonicWALL ファイアウォールを使ってワンアーム モードで配備される、SonicWALL WXA シリーズ装置のサポートを提供します。WAN 高速化装置は、TCP 高速化とウィンドウズ ファイル共有 (WFS) 高速化といった技術を使用して、VPN または 専用リンクで接続された複数箇所間の WAN トラフィックを最適化します。この配備では、SonicWALL 装置は、WAN 高速化装置が余分なトラフィックを排除してプロトコル待ち時間を排除する一方、アプリケーション制御、侵入防御、アンチマルウェア防御、VPN、ルーティング、アンチスパム、およびコンテンツフィルタといった、ネットワーキングおよびセキュリティ サービスを提供します。次の図は、SonicWALL WXA シリーズ装置と SonicWALL ネットワーク セキュリティ装置に対する基本的なネットワーク トポロジを示します。



SonicWALL WXA シリーズ装置を使った WAN 高速化は、高品質のサービスや大きな帯域幅供給を購入することなく、アプリケーション実行応答時間の改善を提供できます。これは、長い待ち時間のためにアプリケーションの不調を引き起こしている WAN 接続で特に注目すべきです。

- **クライアントに複数のプロポーザルを許可するオプション** - 「**クライアントに複数のプロポーザルを許可する**」チェックボックスにより、異なるセキュリティ ポリシーを使う複数の VPN または L2TP クライアントが、SonicOS 5.8.0.3 以上で動作中のファイアウォールに接続することが可能になります。

このオプションは、SonicOS の「**VPN > 設定**」ページから GroupVPN を設定する際の「**詳細**」タブにあります。



クライアント ポリシーは、プロポーザル タブで設定されたプロポーザルに対して、SonicWALL GVC で接続するクライアントと同様に、厳密に確認されることは変わりません。このオプションは GVC には効果がありません。

この「**クライアントに複数のプロポーザルを許可する**」オプションを選択した場合は、SonicOS は、アップル OS、ウィンドウズ、または Android クライアントといった、提示するプロポーザルがプロポーザル タブ上で設定されたものとは異なる他の L2TP クライアントからの接続を許可するようになります。プロポーザルは、以下の条件に一致する場合に受諾されます。

- 提示されたアルゴリズムが、SonicOS で利用可能なアルゴリズムの 1 つと一致する場合
- 提示されたアルゴリズムが、SonicOS プロポーザルで設定されたアルゴリズムよりも強力で安全な場合

このオプションが選択されない場合は、SonicOS はクライアントが設定されたポリシーと厳密に一致することを要求します。このオプションにより、SonicWALL は、アップル、ウィンドウズ、および Android クライアントのための混成環境をサポートできるようになります。このオプションを使って、SonicOS はこれらのクライアントが持つプロポーザルが SonicOS でサポートされるアルゴリズムの組み合わせを含み、ポリシー内で GVC といった他のクライアントの失敗を防ぐように設定されていない場合に、これらのクライアントと動作できます。

- **ゲートウェイ アンチウィルスの強化（クラウド GAV）** - クラウド ゲートウェイ アンチウィルス機能は、危険なマルウェア実例数の継続成長に対抗するために、SonicWALL ファイアウォール上で提供されている既存のゲートウェイ AV 走査メカニズムを引継いで拡張する、高度なマルウェア スキャン対策を導入します。クラウド ゲートウェイ アンチウィルスは、データセンター ベースのマルウェア分析サーバに問い合わせることによって、再組み立て自由な精密パケット検査能力を拡張します。このアプローチは、現在どんな大きな処理オーバヘッドの増加も装置自身に加えずにサポートされるすべてのプロトコルで、無制限なサイズの無制限な数のファイルをスキャン可能な、遅延の少ないのリアルタイム ソリューションを提供することによって、RFDPI ベースのマルウェア検出の基礎を保ちます。この追加レイヤのセキュリティにより、SonicWALL の 次世代ファイアウォールは現在の保護を拡張して数百万ものマルウェア要素をカバーすることができます。
- **NTP 認証種別** - ネットワーク タイム プロトコル サーバの追加時に、NTP サーバの追加ダイアログボックスで、MD5 などの NTP 認証種別を指定するフィールドが提供されます。また、信頼鍵番号、鍵番号、そしてパスワードを指定するためのフィールドも利用可能です。
- **コンテンツ フィルタの拡張** - CFS の拡張により、アプリケーション使用、ユーザ アクティビティ、そしてコンテンツ種別に基づいたネットワーク トラフィックのポリシー管理が提供されます。管理者は、ユーザ グループ毎に、複数の CFS ポリシーを作成して、CFS 種別に基づいた制限の '帯域幅管理ポリシー' を設定できます。
- **TZ シリーズの VLAN サポート** - SonicOS 5.8 は、SonicWALL TZ 105/205 シリーズ装置に対する VLAN サポートを提供します。
- **TZ シリーズの SonicPoint 仮想アクセス ポイント サポート** - SonicWALL TZ 105/205 シリーズ装置に 1 台以上の SonicPoint が接続されている場合に、仮想アクセス ポイント（VAP）がサポートされます。
- **LDAP プライマリ グループ属性** - ポリシー設定時にドメイン ユーザを使うことを許可するために、"プライマリ グループ" 属性を通してドメイン ユーザ グループのメンバーシップが検索可能です。この機能を使うために SonicOS 5.8.1.7 は LDAP スキーマ設定内の属性設定を提供します。
- **アップグレード後のアンチウィルス除外の維持** - SonicOS 5.8.1.7 は、開始 IP アドレスが、LAN、WAN、DMZ、または WLAN ゾーンのどれかに属するアンチウィルス執行から除外するために設定された既存の範囲内かどうかを検知する機能を提供します。新しいファームウェア バージョンにアップグレードした後で、SonicWALL はこの IP 範囲を新しく作成されたアドレス オブジェクトに適用します。個別ゾーンを含む、上記にリストされていない他のゾーンのアドレスの検知はサポートされません。

アップグレードの前に存在していて個別ゾーン内にあるホストに適用されていたアンチウィルス除外は、検知されません。サポートされているゾーン内に無い IP アドレス範囲は、LAN ゾーンに戻ります。LAN ゾーンへの変換は、再起動処理中に実行されます。SonicWALL 管理インターフェースへのログイン時に、この変換に関するメッセージは表示されません。

- **統合アンチスパム サービス (CASS) 2.0** - 統合アンチスパム サービス (CASS) 機能は、SonicWALL セキュリティ装置にアンチスパム、アンチフィッシング、そしてアンチウィルス能力を追加するための、素早く能率的で、効果的な手法を提供します。この機能はユーザ表示設定を構成してジャンク メッセージをユーザがインボックス内で見る前に

フィルタする機能を提供することで、SonicWALL セキュリティ装置の能力を増大します。CASS 2.0 では、以下の拡張が利用可能になりました。

- Email Security ジャンク ストア アプリケーションを、Exchange サーバ システムの外部 (例えばリモート サーバ上) に配備可能です。
- ジャンク ストア ユーザ インターフェース ページの機能により、ジャンク ストアが SonicOS の左側ナビゲーション ペインのアンチスパム下に表示するページ一覧を SonicOS に通知できます。たとえば、ペインはジャンク ボックスの表示、ジャンク ボックスの設定、ユーザ表示設定、かつ/またはアドレス ブックを表示することができます。
- ホスト オブジェクトに加えて、FQDN と範囲オブジェクトと共にユーザ定義の許可および拒否リストが設定できます。
- 「アンチスパム > 状況」ページで、GRID IP の確認ツールが利用可能です。SonicWALL 管理者は IP アドレスを指定 (必要時に) して、SonicWALL GRID IP サーバで調べ合わせることができます。この結果は、リストされている、いないで返されます。リストされているホストからの接続は、CASS が動作している SonicWALL セキュリティ装置によって（許可リストで優先されない限り）遮断されます。
- 「アンチスパム > 設定」ページの詳細オプション セクションで、プローブ応答のタイムアウトを指定するパラメータが利用可能です。このオプションは、ターゲットが頻繁に利用不可とマークされることを防ぐために、より長いタイムアウトが必要な配備シナリオをサポートします。既定値は 30 秒です。

- **接続制限の拡張** - 接続制限の拡張は、それぞれの IP アドレスに対する接続数の包括的制御を提供していた最初の接続制限機能を広げます。この拡張は、SonicWALL 管理者がより柔軟に接続制限を設定できるように、この種の制御の細やかさを増強するように設計されています。接続制限は、接続制限を設定する際に、管理者が IP アドレス、サービス、およびトラフィック方向を選ぶことを許可するために、ファイアウォール アクセス ルールとポリシーを使用します。
- **動的 WAN スケジュール** - SonicOS 5.8 は、動的 WAN クライアントがいつ接続できるかを制御するためのスケジューリングをサポートします。動的 WAN クライアントは、PPPoE、L2TP、または PPTP を使って WAN インターフェースに接続し、IP アドレスを取得します。この拡張で管理者は、動的 WAN クライアントにスケジュールオブジェクトを紐付けて、スケジュールが許可する時間に接続を許可して、設定されたスケジュールの終わりで切断することができます。SonicOS 管理インターフェースでは、IP 割り当てに対して前述のプロトコルの 1 つが選択されている場合に、WAN インターフェースの設定画面でスケジュール オプションが利用可能です。一旦スケジュールが適用されると、スケジュールの開始と停止時にログ イベントが記録されます。
- **Mozilla ブラウザでの NTLM 認証** - シングル サインオン拡張の 1 つとして、SonicOS は Mozilla ベースのブラウザを使ってブラウズするユーザを識別するために NTLM 認証を使えるようになりました (インターネット エクスプローラ、Firefox、Chrome、Safari を含む)。NTLM は、“統合ウィンドウズ セキュリティ” として知られるブラウザ認証スイートで、すべての Mozilla ベースのブラウザでサポートされるべきです。これにより、SonicWALL 装置からブラウザに対して SSO エージェントの関与無しで直接認証要求ができます。NTLM 認証はウィンドウズ、Linux、および Mac PC 上のブラウザで動作して、SSO エージェントと協調動作することのできない Linux と Mac PC のシングル サインオンを実行するメカニズムを提供します。
- **シングル サインオンのユーザを LDAP からインポートするオプション** -「ユーザ > ローカル ユーザ」ページの「**LDAP からインポート**」ボタンにより、LDAP サーバからユーザ名を取得することで SonicWALL 上のローカル ユーザを設定できます。これにより、成功した LDAP 認証を経て SonicWALL のユーザ権限を容認することができます。容易に使えるように、リストを管理可能なサイズに縮小してからインポートするユーザを選択するオプションが提供されます。
- **SSL VPN NetExtender 更新** - この拡張は、様々な修正と共に、SSL VPN ユーザによるパスワードを変更機能をサポートします。パスワードの期限が切れる場合、NetExtender クライアントか SSL VPN ポータルを介してログインするときに、ユーザにパスワード変更が要求されます。これはローカル ユーザとリモート ユーザーの両方 (RADIUS と LDAP) をサポートします。
- **DHCP スケーラビリティの拡張** - SonicWALL 装置の DHCP サーバは、以前サポートしていたリース数の 2 倍から 4 倍を提供するように拡張されました。DHCP インフラのセキュリティを強化するために、SonicOS DHCP サーバは、ネットワーク上に割り当てられた IP アドレスを使っている別の機器が無いことを確認するために、サーバ サイドの競合検出を提供するようになりました。競合検出は、アドレスを取得時の遅延を避けるために非同期に実行されます。

- **SIP アプリケーション レイヤ ゲートウェイの拡張** - SonicOS 5.8 で、SIP 動作と能力の拡張が提供されます。この SIP 機能セットは、以前の SonicOS リリースと同等のままですが、大幅に強化された信頼性とパフォーマンスを提供します。「VoIP > 設定」ページの「SIP の設定」セクションは変更されていません。

SonicOS ファームウェアには、古いプラットフォーム上の非常に古いバージョンから、SIP ALG サポートが存在しています。SIP ALG の変更は、電話機の間で最適化された中間物、SIP Back-to-Back User Agent (B2BUA)、追加の機器ベンダ、そしてマルチコア システム上での動作をサポートするために、時間の経過とともに追加されています。

VoIP を含む音声インフラを保護する SIP プロトコルは、現在商業上非常に重要な位置付けになりました。この現代の音声インフラの要求に順応するために、SIP ALG 拡張は以下を含みます。

  - **SIP エンドポイント情報データベース** - 既知のエンドポイントの状況情報を維持するこのアルゴリズムは、強化されたパフォーマンスと拡張性のためにデータベースを使うように再設計されました。エンドポイント情報はユーザ ID に紐付けられなくなり、単一のエンドポイントに複数のユーザ ID を関連付けることが可能になりました。NAT ポリシー、またエンドポイント IP アドレスとポートによる索引付けを使うエンドポイント データベース アクセスは、柔軟で効率的です。
  - **自動追加される SIP エンドポイント** - ユーザにより設定されたエンドポイントは、ユーザにより設定された NAT ポリシーに基づいて、これらのエンドポイントが "学習済み" ではなく事前設定済みとして自動的にデータベースに追加され、強化されたパフォーマンスを提供し、正しいマッピングを確かにします。
  - **SIP 通話データベース** - 進行中の通話についての情報を維持するための通話データベースが実装され、強化されたパフォーマンスと拡張性を提供し、SonicOS がより多くの同時通話を処理することを可能にします。通話データベース エントリは、複数通話と関連付けることが可能です。
  - **B2BUA サポートの拡張** - SIP Back-to-Back User Agent サポートは、様々なアルゴリズムの強化があり、より効率的です。
  - **接続キャッシュの強化** - 以前に接続キャッシュで保持されたデータの多くが、エンドポイント データベースか通話データベースのどちらかにオフロードされ、より効率的なデータ アクセスとそれに伴う性能の強化につながります。
  - **正規シャットダウン** - ファイアウォールの再起動の要求や既存の SIP エンドポイントと通話状態情報のタイムアウトを待つことなく、SIP 変換を無効にすることを可能にします。
- **ネットワーク インターフェースに対する管理トラフィックのみのオプション** - SonicOS 5.8.1.7 は、「ネットワーク > インターフェース」ページからインターフェースを設定する際に、インターフェースの設定ウィンドウの「**詳細**」タブに、「**管理トラフィックのみ**」オプションを提供します。選択すると、このオプションはインターフェースに到着するすべてのトラフィックに優先順位をつけます。管理者は、完全に管理目的で使うように計画されたインターフェースに対してのみ、このオプションを有効にするべきです。通常のインターフェースでこのオプションが有効な場合でも、トラフィックに優先順位付けされますが、期待した結果になりません。トラフィックを管理のためだけに制限するのは、管理者次第であり、ファームウェアには通過するトラフィックを防ぐ能力はありません。

このオプションの目的は、装置が 100% の使用率で動作している場合でも SonicOS 管理インターフェースにアクセスする手段を提供するためです。

- **ユーザ認証をバイパスさせる URL の自動設定** - SonicOS 5.8.1.7 には、単一の特定の IP アドレスからのトラフィックを認証をバイパスして一時的に許可するための自動設定ユーティリティがあります。トラフィックがアクセスする宛先は記録され、トラフィックがユーザ認証をバイパスすることを許可するために使われます。通常これはアンチウィルスの更新やウィンドウズ アップデートのようなトラフィックを許可するために使われます。この機能を使うには、「**ユーザ > 設定**」ページに移動して「その他のグローバル ユーザ設定」セクションの、「**自動設定**」ボタンを選択します。

確認されている問題点

以下は、SonicOS 5.8.1.7-5o+ で確認されている問題点です。

アプリケーション制御

概要	背景 / 応急	問題
アプリケーション ルール ポリシーが添付ファイルを遮断するように作成されていても、添付ファイル付きの電子メールを受信します。	アプリケーション ルール ポリシーが .exe の添付ファイルを持つ POP3 着信電子メールを遮断するように作成されていて、PC から ファイアウォールの LAN インターフェースに接続して .exe の添付ファイルを持つ電子メールを送信した場合に発生します。	111851
アプリケーション制御詳細ポリシーが WAN ゾーンではなく、VPN ゾーンとのトラフィックに適用されます。	WAN ゾーン上でアプリケーション制御サービスが有効になっていて、すべてのシグネチャに対してログまたは遮断動作が有効になっている場合に発生します。LAN から VPN へのトラフィックが生成されると、アプリケーション制御詳細ポリシーが VPN トラフィックに適用されます。	107296
グローバルに無効にしても、アプリケーション ルール ポリシーの効果が継続します。	ポリシーをグローバルに無効にするために「**アプリケーション ルールを有効にする**」チェックボックスを非選択にしてからアプリケーション ルールポリシーを作成した場合に発生します。WAN インターフェース上のトラフィックがこのルールに一致すると、設定されたポリシー動作が適用されます。**応急**:「**アプリケーション ルールを有効にする**」チェックボックスを非選択にしてから装置を再起動します。	101194

帯域幅管理

概要	背景 / 応急	問題
インターフェースに対する受信または送信値が編集されて、トラフィックがそのインターフェースを通過する際にトラフィックが落とされます。	インターフェースがトラフィックを通過させている間に、受信または送信インターフェース値を編集した場合に発生します。 **応急**: インターフェース上のトラフィックを停止してから、値を編集します。	101286
帯域幅管理のアプリケーション ルールが、誤ったグローバル BWM 優先順位キューにマップされることがあります。	「**アプリケーション フロー監視**」ページで帯域幅管理ルールを作成して、優先順位を「**高**」に設定した場合に発生します。「**アプリケーション フロー監視**」ページには、「**高**」優先順位を選択して作成されたルールにも関わらず、「**中**」の優先度設定で表示されます。	100116

高可用性

概要	背景 / 応急	問題
WAN フェイルオーバーとフェイルバックにより、インターネット接続問題が発生することがあります。	WAN 負荷分散を使用していて、ICMP または TCP を使って監視している NAT 静的 IP アドレスに対しての監視が失敗した場合に発生します。	112783

ログ

概要	背景 / 応急	問題
ターミナル サーバからの接続に対する Syslog メッセージ内に SonicWALL によってユーザ名が生成されません。その結果 ViewPoint のレポートにユーザ名が含まれません。	ユーザが接続した後、しかしその接続に対するユーザの識別情報が TS エージェントから受信される前にターミナル サーバからのトラフィックに対する Syslog メッセージが送信された場合に発生します。	89488

ネットワーク

概要	背景 / 応急	問題
ルート ベースの VPN またはトンネル インターフェースに対して断続的にルートが落ちます。	OSPF が有効なリモート機器に向けて 2 つ以上のルート ベースの VPN (またはトンネル インターフェース) が構成されている場合に発生します。	102961

セキュリティ サービス

概要	背景 / 応急	問題
いくつかのバージョンの UltraSurf が SonicOS 侵入防御サービスによって、ログ メッセージには接続が遮断されたと記載されているにも関わらず遮断されません。	UltraSurf 11.03 または 11.04 がファイアウォール ポリシーをバイパスするために使用されている場合に発生します。**応急**: DPI-SSL を有効にして、65.49.14.0/24 サブネットへのすべての UDP トラフィックを (アクセス ルールを用いて) 遮断します。	111716
SonicOS 5.6.0.x から 5.8.x にアップグレードした後で、アンチウィルス強制リストが正しくありません。	SonicOS 5.6.0.x 上で Kaspersky アンチウィルスがライセンスされ、ゾーンに対して有効な AV 強制とセキュリティ サービス ページ上で設定された AV 強制リストがあった場合に発生します。	110845

システム

概要	背景 / 応急	問題
VLAN インターフェースの追加後に、ファイアウォールが特異な許可されたトラフィックの転送を停止します。	VLAN サブ インターフェースが追加された場合に、2 台の異なる NSA 4500 装置上で発生します。施行されているファイアウォール ルールのために、パケットが破棄されます。**応急**: VLAN インターフェースを追加した後で、特異なトラフィックを許可するポリシーを無効にしてから有効にします。	114206

ユーザ

概要	背景 / 応急	問題
ホストへの Ping やドメイン名を使ったウェブサイトへのアクセス後に、ログ ページがメッセージ “UDP Packet Dropped” を表示します。	「ユーザ ＞ 設定」ページに移動して、「**シングル サインオン方法**」ドロップダウン リストで「**SSO エージェント**」を選択してから、TSA エージェントを設定して、既定の LAN から WAN へのアクセス ルールのユーザを「**Trusted Users**」に設定した場合に発生します。	111879

ユーザ インターフェース

概要	背景 / 応急	問題
DHCP の設定を編集しているときに、JavaScript エラーが表示されることがあります。	DHCP オプション グループを編集しているとき、またはインターフェース設定を編集して DHCP スコープを変更しているときに発生します。	110087

VPN

概要	背景 / 応急	問題
ときどき、セカンダリ IPSec ゲートウェイが、プライマリ ゲートウェイが到達不能の場合にピアとのトンネル確立ができなくなります。	2 台の SonicWALL 装置間で 1 つ IPSec VPN トンネルが設定されていて、そのうち 1 台が二重 WAN インターフェース (X1 と X4) を持っている場合に発生します。プライマリ WAN インターフェースが切断されると、セカンダリ インターフェースを使ってトンネルを確立できません。	103935

日本語版特有の問題点

概要	背景 / 応急	問題
「ダッシュボード ＞ 接続監視」ページでエクスポートした CSV 形式の接続監視結果ファイルをエクセルで開くと、文字化けすることがあります。	エクセルが UTF-8 エンコードの CSV ファイルを異なるエンコードで開くために発生し、ヘッダ行 (1 行目) が文字化けします。**応急**: 最初にテキスト エディタ等で CSV ファイルのエンコードを Shift-JIS または BOM 付きの UTF-8 に変更してから、エクセルで開きます。	-
「システム > 管理」ページから言語を切替えると、設定情報が破損することがあります。	本リリースのファームウェアは、設定を引き継いだ言語の切替をサポートしていません。 日本語から英語に切替えて、その後日本語に戻しても設定情報は破損した状態になるので、言語を切替えないでご利用ください。**応急**: 言語を切替えてしまった場合は、工場出荷時の設定で起動してから、必要な設定を行ってください。	-
「システム > 設定」ページからファームウェアをアップロードし、“アップロードされたファームウェア”で起動すると、通常表示されるはずの再起動中の画面が正しく表示されないことがあります。	インターネット エクスプローラを使用して“アップロードされたファームウェア”で起動した場合に発生します。この問題が発生しても、機器は正しく再起動されます。**応急**: インターネット エクスプローラの代わりにFireFoxを使用します。	-

「セキュリティ サービス > 概要」ページが正しく表示されないことがあります。	「プロキシを経由しての手口ダウンロード」機能を有効にした場合に発生します。この問題が発生しても、手口のダウンロード機能は正しく動作します。	83453
SSL VPN ポータルにログイン後、NetExtender ボタンを選択しても SSL VPN 接続に失敗することがあります。	日本語版ウィンドウズ XP を使用した場合に発生し、NetExtender のインストールは完了していますが接続に失敗することがあります。**応急**: 接続の失敗後に、PC を再起動してから再度 SSL VPN ポータルで NetExtender ボタンを選択します。	-
本リリースのファームウェアは、工場出荷時の設定で起動してから一度も英語表示の管理画面に切替えていない 5.x ファームウェアからのみ、設定を引き継いだアップグレード、およびエクスポートした設定ファイルのインポートに対応しています。それ以外の状況での設定の引き継ぎとインポートにはまだ対応していません。	今後のパッチ リリースで対応する予定です。	-
管理画面やメッセージに、英語で表示される箇所があります。	-	-

修正された問題点

以下は、SonicOS 5.8.1.7-5o+ で修正された問題点です。

コンテンツ フィルタ システム

概要	背景 / 応急	問題
「セキュリティ サービス ＞ コンテンツ フィルタ」ページ上のエントリ削除試行が失敗して、状況ラインにエラー メッセージ “不正な値です。スクリプトに似た文字列が見つかりました” が表示されます。	「セキュリティ サービス ＞ コンテンツ フィルタ」ページ上の「**遮断時に表示するウェブ ページ**」テキスト ボックスが HTML テキストを含んでいる状況で、「**信頼されたドメイン**」リストまたは「**IP アドレス範囲での CFS ポリシー**」リストからエントリの削除を試みた場合に発生します。**応急**: 「**遮断時に表示するウェブ ページ**」内のすべてのテキストを (どこかに保存してから) 削除し、ポリシー エントリを削除してから、遮断メッセージのテキストを追加しなおします。	115129

ファームウェア

概要	背景 / 応急	問題
以前にカスタマイズされたログイン認証ページを使って、ファイアウォールの管理インターフェースにログインできません。	SonicOS 5.8.1.6-3o+ ファームウェアが稼動している管理インターフェースに、SonicOS 5.8.1.5-46o+ 以前で作成したユーザ定義ログイン認証ページを使ってログインした場合に発生します。**応急**: もし現在のログイン認証ページが管理インターフェースへのアクセスを許可していない場合は、“defauth.html” を使ってログインします。「**ユーザ ＞ 設定**」ページに移動して、「**ログイン ページのユーザ定義**」セクションで「**既定**」ボタンを選択します。このテンプレートを使って管理インターフェースのログイン認証ページをカスタマイズしてから、「**適用**」ボタンを選択します。	114699
トンネル インターフェース VPN ポリシーを使う場合の安定性の改良が必要です。	X0 上で OSPF が有効で、約 130 のトンネル インターフェース種別の VPN SA が使用中の場合に発生します。	113886
スタンドアロン モードまたは高可用性ペアの構成で、ファイアウォールが不定期に再起動することがあります。	SonicWALL NSA 2400 セキュリティ装置上で SonicOS ファームウェアをアップグレードした後に発生します。	113445

ネットワーク

概要	背景 / 応急	問題
NAT ポリシー ルックアップが、誤ったメッセージを生成することがあります。	ルックアップが “CRITICAL - Informational: natPolicyRemap:1282:” を含むメッセージを生成した場合に発生します。	114478

SonicOS イメージのアップグレード手順

以下の手順は、既存の SonicOS イメージを新しいバージョンへアップグレードする方法について説明しています。

最新版 SonicOS イメージの取得

SonicWALL セキュリティ装置の新しい SonicOS ファームウェア イメージを入手するには、以下の手順に従います。

1. mySonicWALL アカウントを用いて http://www.mysonicwall.com に接続します。
2. 新しい SonicOS イメージ ファイルを管理ステーションへコピーします。

LAN インターフェースまたは WAN インターフェースへの管理アクセスを設定している場合、SonicWALL セキュリティ装置上の SonicOS イメージをリモートで更新することができます。

設定情報のバックアップ コピーの保存

アップグレード処理を開始する前に、SonicWALL セキュリティ装置の設定情報のシステム バックアップを作成します。バックアップ機能は、SonicWALL セキュリティ装置上の現在の設定情報のコピーを保存し、以前の設定状態へ戻るために必要となるすべての既存の設定情報を保護します。

SonicWALL セキュリティ装置の現在の設定状態を保存するためにバックアップ機能を使用することに加えて、設定情報ファイルを管理ステーションのローカル ハードディスクへエクスポートすることができます。このファイルは、設定情報の外部バックアップとして利用でき、SonicWALL セキュリティ装置へインポートすることができます。

設定情報のバックアップの保存、および、ファイルを管理ステーションへエクスポートするには、以下の手順に従います。

1. 「システム > 設定」ページの「バックアップの作成」ボタンを選択します。システム バックアップ エントリが「ファームウェアの管理」テーブルに表示されます。
2. 設定情報ファイルをローカル マシンに保存するには、「設定のエクスポート」ボタンを選択します。ポップアップ ウィンドウに、セーブされたファイル名が表示されます。
3. 「システム > 診断」ページの「テクニカル サポート レポート」セクションで、以下のチェックボックスを選択してから「**レポートのダウンロード**」ボタンを選択します。

- VPN 鍵
- ARP キャッシュ
- DHCP バインディング
- IKE 情報
- SonicPointN 診断

- 現在のユーザ
- ユーザ詳細

これらの情報が、あなたの管理コンピュータ上の “techSupport_” ファイルに保存されます。

現在の設定を使用した SonicOS イメージのアップグレード

SonicWALL 装置に新しいファームウェアをアップロードして、現在の設定を使用して起動するには、以下の手順に従います。

1. mySonicWALL より SonicOS イメージ ファイルをダウンロードし、ローカル コンピュータ上に保存します。
2. 「システム > 設定」ページより、「ファームウェアのアップロード」を選択します。
3. ローカルに保存しておいた SonicOS ファームウェア イメージ ファイルを選択し、「アップロード」を選択します。
4. 「システム > 設定」ページから、「アップロード されたファームウェア」エントリの起動アイコンを選択します。
5. 確認のダイアログ ボックスが表示されます。「OK」を選択して継続します。SonicWALL は再起動してログイン画面が表示されます。
6. ユーザ名とパスワードを入力します。新しい SonicOS イメージのバージョン情報は、「システム > 設定」ページで確認できます。

SonicOS 5.8 への設定ファイルのインポート

SonicWALL ネットワーク セキュリティ装置へインポートできる設定ファイルは、SonicOS が動作している以下の SonicWALL 装置からのものをサポートします

- NSA シリーズ
- NSA E-Class シリーズ
- TZ 210/200/100/190/180/170 シリーズ
- PRO シリーズ

SonicOS Enhanced 5.8 が動作しているこれらの装置へインポートできる設定ファイルで一部例外があります。以下の場合、設定ファイルをインポートできません

- 設定ファイルに SonicOS 5.x 以前に作成された Portshield インターフェースが含まれる場合。
- 設定ファイルに TZ 100/200 シリーズが受け付けない VLAN インターフェースが含まれる場合。
- VLAN インターフェースが作成された光ファイバー インターフェースを持つ PRO 5060 からの設定ファイルの場合。

これらの装置からの設定のインポートの完全なサポートは、今後のリリースで予定されています。その際は、MySonicWALL 上で利用可能になった SonicOS の最新のメンテナンス リリースにファームウェアをアップグレードする必要があります。

SonicOS Standard から SonicOS 5.8 Enhanced への設定ファイルのインポート

SonicOS Standard から Enhanced への設定コンバータは、元の Standard ネットワーク設定ファイルを、対象の SonicOS Enhanced 装置と互換性があるように置換するために設計されています。より高度な SonicOS Enhanced の機能のために、そのネットワーク設定ファイルは SonicOS Standard で使われるものよりも複雑です。それらは非互換です。この設定コンバータは、元の Standard の設定ファイルをベースにして、Enhanced を対象として完全に新しいネットワーク設定ファイルを作成します。これにより、ネットワーク ポリシーの再作成により時間を消費せずに Standard から Enhanced への素早いアップグレードが可能です。**補足** SonicWALL は、まず試験環境で対象の変換されたネットワーク設定ファイルを配備することと、常に元の変換前のネットワーク設定ファイルのバックアップ コピーを保管することを推奨します。

SonicOS Standard から Enhanced への設定コンバータは、https://convert.global.sonicwall.com/ で利用できます。

設定の変換に失敗した場合は、SonicOS Standard 設定ファイルに問題の簡単な説明を添えて、settings_converter@sonicwall.com に送信してください。この場合、SonicWALL 装置を手作業で設定することも考慮してください。

Standard ネットワーク設定ファイルを Enhanced 用に変換するには、

1. SonicOS Standard 装置の管理インターフェースにログインし、**システム > 設定** に移動します。そしてネットワーク設定を管理コンピュータ上のファイルに保存します。
2. 管理コンピュータ上で、ブラウザで https://convert.global.sonicwall.com/ に移動します。
3. **Settings Converter** ボタンを選択します。
4. あなたの MySonicWALL 資格情報を用いてログインし、セキュリティ声明に同意します。

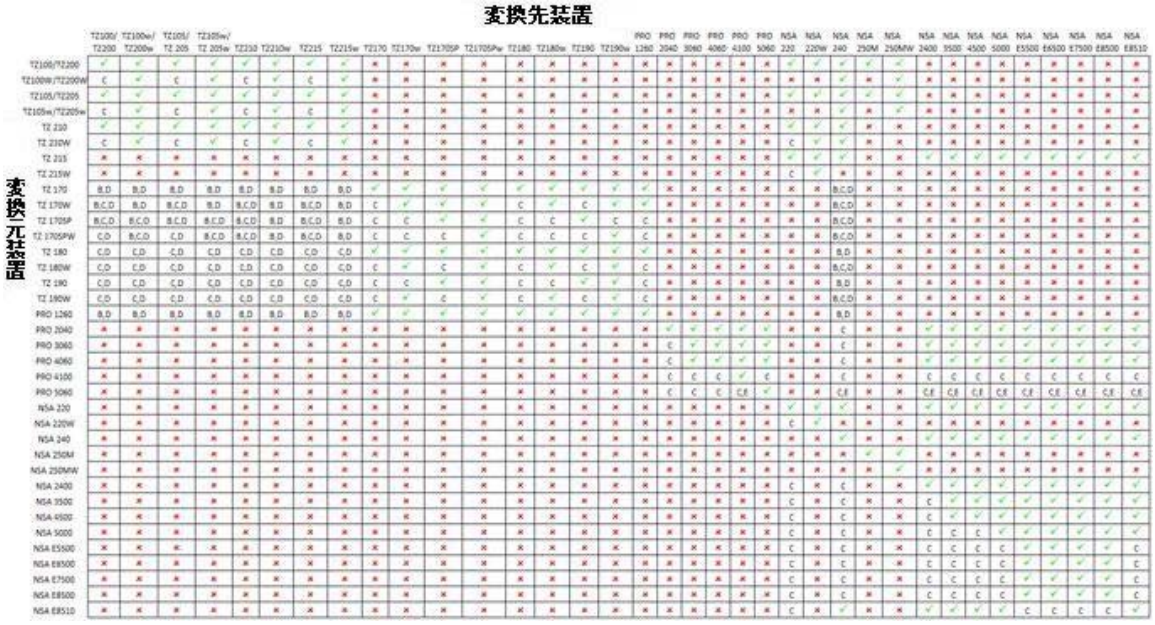
   変換プロセスの中で、Standard ネットワーク設定ファイルを MySonicWALL にアップロードする必要があります。設定変換ツールは MySonicWALL の認証を使い、ユーザのネットワーク設定を保護します。ユーザは、変換プロセスの完了後も SonicWALL がユーザのネットワーク設定のコピーを保持するということを理解する必要があります。
5. Standard ネットワーク設定ファイルをアップロードします。
   - **Browse** を選択します。
   - 変換元の SonicOS Standard 設定ファイルを探して選択します。
   - **Upload** を選択します。
   - 右矢印を選択して継続します。
6. 変換元の SonicOS Standard 設定概要ページを確認します。

   このページは、アップロードした変換前のネットワーク設定ファイルに含まれる有用なネットワーク設定情報を表示します。試験目的で、試験環境に配備するためにこのページ上で装置の LAN IP とサブネット マスクを変更できます。
   - (オプション) 変換元の装置の IP アドレスとサブネット マスクを変換先の試験用装置に合わせて変更します。
   - 右矢印を選択して継続します。
7. 利用可能なリストから、Enhanced を配備する変換先の SonicWALL 装置を選択します。

   様々な SonicWALL 装置で、主にサポートするインターフェースの数が異なることから、SonicOS Enhanced は異なる設定がなされます。そのように、配備する対象装置のために、変換された Enhanced ネットワーク設定ファイルはカスタマイズされる必要があります。
8. 右矢印を選択して継続し変換を完了します。

9. オプションで、**Warnings** リンクを選択することで変換先の装置に対して生成された設定の相違点を参照できます。
10. **Download** ボタンを選択して、保存を選択することで、管理コンピュータ上に新しい変換先の SonicOS Enhanced ネットワーク設定ファイルを保存します。
11. SonicWALL 装置の管理インターフェースにログインします。
12. **システム > 設定** ページに移動し、**設定のインポート** ボタンを選択して、変換された設定を装置にインポートします。

設定のインポートに関するサポート表



補足：
A – VLAN が存在する場合は、設定ファイルは受諾されません。
B – SonicOS 5.x 以前の Portshield インターフェースはサポートされません。
C – 超過分のインターフェースからの設定情報は削除されます。NAT ポリシーやファイアウォール アクセス ルールとその他インターフェースに依存する設定も削除されます。
D – SonicOS 5.x 以外の機器からのインポート時には、X2 インターフェースは DMZ ゾーン内に設定されます。
E – 光インターフェースのサブインターフェースとして作成された VLAN は削除されます。

✓ サポートされます。

× サポートされません。設定ファイルのインポートは成功しますが、ファイアウォールの制限により、DHCP スコープ、VPN 設定、その他の設定が削除されます。

工場出荷時の設定を使用した SonicOS イメージのアップグレード

以下の手順を実行して、SonicWALL 装置に新しいファームウェアをアップロードして、既定の設定で起動します。

1. mySonicWALL より SonicOS イメージ ファイルをダウンロードし、ローカル コンピュータ上に保存します。
2. 「システム > 設定」ページより「バックアップの作成」を選択します。
3. 「ファームウェアのアップロード」を選択します。
4. ローカルに保存しておいた SonicOS ファームウェア イメージ ファイルを選択し、「アップロード」を選択します。
5. 「システム > 設定」ページから、「アップロード されたファームウェア (工場出荷時の設定) 」エントリの起動アイコンを選択します。
6. 確認のダイアログ ボックスが表示されます。「OK」を選択して継続します。SonicWALL は再起動して、ログイン画面へのリンクがあるセットアップ ウィザードが表示されます。
7. 既定のユーザ名とパスワード (admin/password) を入力して、SonicWALL 管理インターフェースにアクセスします。

セーフモードを使用したファームウェアのアップグレード

セーフモードの手順は、小さい穴の中のリセット ボタンを使います。この場所は様々で、NSA モデルでは、ボタンは前面の USB ポートの近くにあり、TZ モデルでは、ボタンは背面の電源コードの隣にあります。SonicWALL セキュリティ装置の管理インターフェースへ接続できない場合、セーフモードで SonicWALL セキュリティ装置を再起動することができます。セーフモード機能は、「システム > 設定」ページと同じ設定が利用可能な簡素化された管理インターフェースを使用して、不確かな設定状態から素早く復旧することを可能にします。

セーフモードを用いて SonicWALL セキュリティ装置のファームウェアをアップグレードするには、以下の手順に従います。

1. SonicWALL 装置の X0 ポートへ管理ステーションを接続し、管理ステーションの IP アドレスを 192.168.168.0/24 のサブネット上のアドレス、例えば「192.168.168.20」に設定します。
2. 装置をセーフモードで再起動するには、次のどちらかを行います。

- 先の尖った細い (まっすぐにしたクリップや爪楊枝のような) 物を使用して、セキュリティ装置前面のリセット ボタンを 20 秒以上押し続けます。
- フロントベゼルの LCD 制御を用いて装置をセーフモードに設定します。選択すると、LCD は確認表示になるので、Y を選択してから Right ボタンを押します。SonicWALL セキュリティ装置はセーフモードに変更されます。

SonicWALL セキュリティ装置がセーフモードで再起動されると、「Test」ライトが点滅します。

備考 *リセット ボタンを 2 秒間押し続けると診断スナップショットをコンソールに送ります。リセット ボタンを 6 から 8 秒間押し続けると装置を通常モードで再起動します。*

3. ウェブ ブラウザで 192.168.168.168 にアクセスします。セーフモード管理インターフェースが表示されます。
4. セキュリティ装置の設定に変更を加えた場合は、「次回起動時にバックアップを作成する」を選択し、現在の設定のバックアップ コピーを作成します。設定は、装置の再起動時に保存されます。
5. 「ファームウェアのアップロード」を選択し、ローカルに保存しておいた SonicOS ファームウェア イメージ ファイルを選択し、「アップロード」ボタンを選択します。
6. 次の起動アイコンのうちのどちらかを選択します。

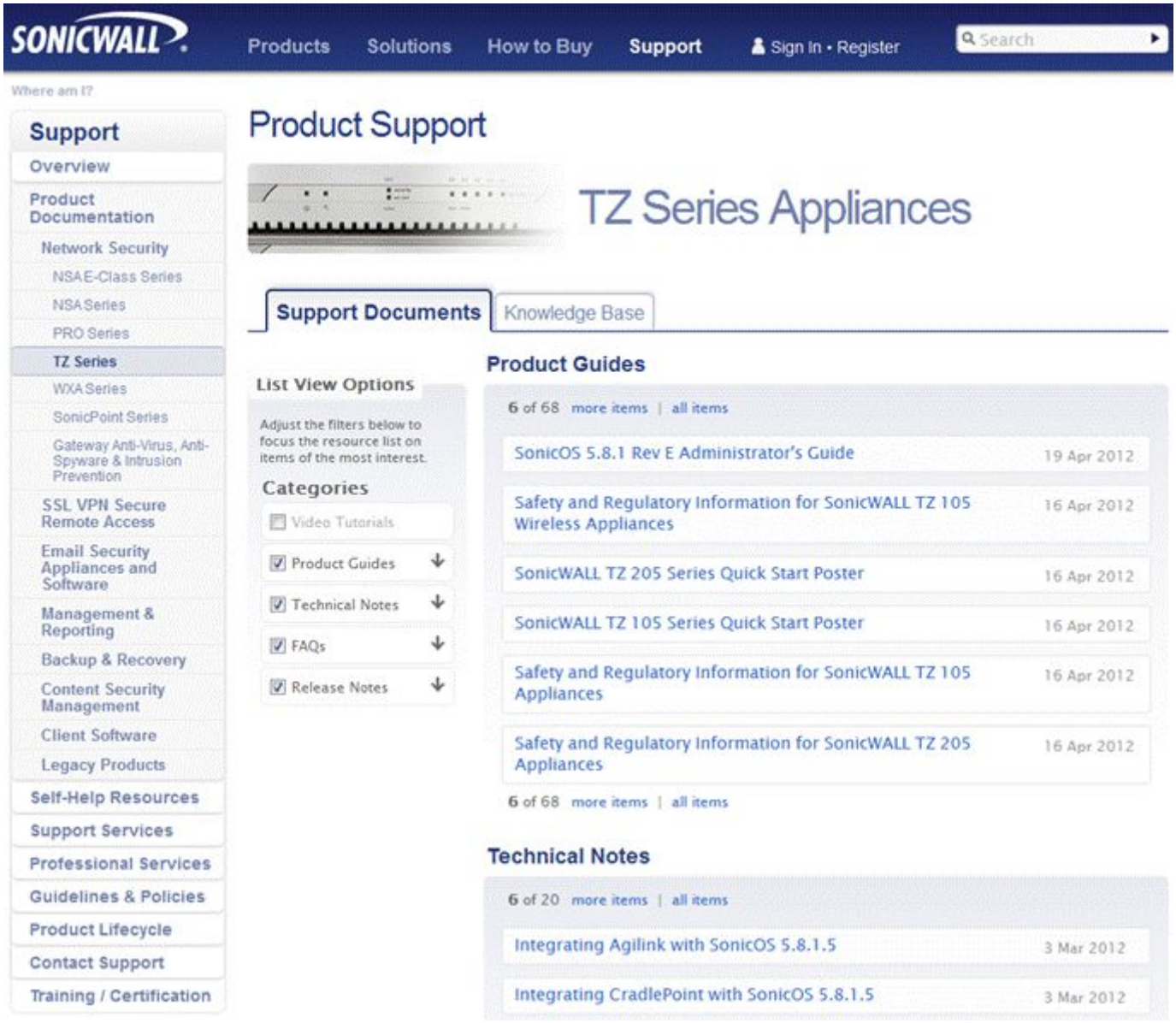
- **アップロード されたファームウェア – 更新!** 
  このオプションを選択すると、装置は現在の設定で再起動します。
- **アップロード されたファームウェア (工場出荷時の設定) – 更新!** 
  このオプションを選択すると、装置は工場出荷時の設定で再起動します。

7. 確認のダイアログ ボックスが表示されます。「OK」を選択して継続します。
8. ファームウェアが正しく起動した後に、ログイン画面が表示されます。工場出荷時の設定で起動した場合には、既定のユーザ名とパスワード (admin/password) を入力して、SonicWALL 管理インターフェースにアクセスします。

関連技術文書

SonicWALL ユーザ ガイド、参照ドキュメントは、SonicWALL 技術文書 オンライン ライブラリ
http://www.sonicwall.com/us/Support.html で公開しています。

基本的及び応用的な配置例は、このウェブサイトで公開されている、SonicOS ガイドまたは SonicOS テックノートを参照してください。



ドキュメント バージョン 2012 年 5 月 25 日