SonicWall® SonicOS 6.5.2.1

リリース ノート

2018 年 8 月

このリリース ノートでは、SonicWall® SonicOS 6.5.2.1 リリースについて説明します。

トピック:

SonicOS 6.5.2.1 について

SonicWall SonicOS 6.5.2.1 は、Dell® N-シリーズ スイッチのサポートを含む 32 以上の新機能を提供するメジャーリリースです。 SonicOS 6.5.2.1 では、新しい NS*a* シリーズ装置のサポートも導入されています。

サポート対象プラットフォーム

SonicOS 6.5.2.1 は、次の SonicWall 装置でサポートされます。

- NS*a* 9650
- NS*a* 9450
- NS*a* 9250
- NS*a* 6650
- NS*a* 5650
- NS*a* 4650
- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- TZ600
- TZ500/TZ500 Wireless
- TZ400/TZ400 Wireless
- TZ300/TZ300 Wireless
- SOHO Wireless

- NS*a* 3650
- NS*a* 2650
- NSA 3600
- NSA 2600

メモ: 本書には、一部の国や地域ではリリースされていないプラットフォーム/バージョンに関する記述が含まれている場合があります。

新しいハードウェア サポート

SonicOS 6.5.2.1 は、以下の新しいハイエンドおよびミッドレンジ ネットワーク セキュリティ装置をサポートします。

- NS*a* 6650
- NS*a* 9250
- NS*a* 9450
- NS*a* 9650

新機能

このセクションでは、SonicOS 6.5.2 で導入された新機能について説明します。

トピック:

- DPI-SSL の強化
- SonicWave 機能
- Dell™ N シリーズ スイッチ サポート
- アプリケーション ベースのルーティング
- 判定動作までのキャプチャ ATP 遮断強化
- DNS シンクホール
- LAN バイパス
- セカンダリ ストレージ デバイスでのファームウェア バックアップ
- グローバル検索の強化
- MGMT インターフェースでの高可用性ハートビート
- 動的ボットネット HTTP 認証
- LHM RESTful API
- URI リスト グループ
- 帯域幅クォータ制御
- フレキシブル記憶装置モジュール サポート
- TACACS+ サポート
- 強化されたユーザ ログイン報告

- WeChat ソーシャル認証
- アクセス ポイント可視化の強化
- LAG に対する VLAN 拡張

DPI-SSL の強化

SonicOS DPI-SSL と DPI-SSH 復号化サービスに、多くの機能が追加されました。

トピック:

- DPI-SSL 個別制御
- アクセス ルールに基づいた DPI-SSL 制御
- TLS 証明書ステータス要求の拡張
- ローカル CRL のサポート
- 強化された DPI-SSL 証明書検証
- ECDSA 系暗号のサポート
- DPI-SSL と CFS HTTPS コンテンツ フィルタの独立稼働
- SSH X11 転送の遮断
- 復号化されたパケットの元のポート番号の保持

DPI-SSL 個別制御

DPI-SSL 個別制御により、全体的ではなくゾーン毎に DPI-SSL を有効にすることができます。 ゾーン毎に DPI-SSL クライアントと DPI-SSL サーバの両方を有効にすることができます。

ゾーン上で DPI-SSL クライアントを有効にするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」に移動します。

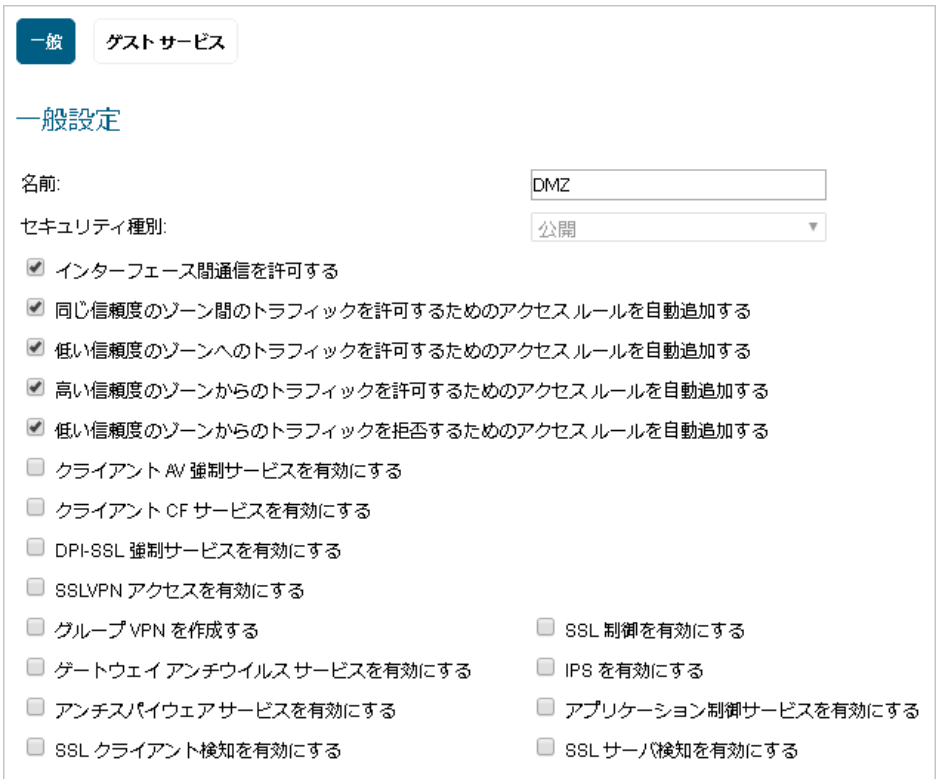
2 「**一般**」を選択します。

3 「**SSL クライアント検査を有効にする**」を選択します。このオプションは既定では選択されていません。

4 「**適用**」を選択して DPI-SSL/TLS クライアントの設定を終了します。

5 「**管理 |システム設定 > ネットワーク > ゾーン**」に移動します。

6 設定するゾーンの「**編集**」アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。



7 「**SSL クライアント検知を有効にする**」を選択します。このオプションは既定では選択されていません。

8 「**OK**」を選択してゾーンの設定を終了します。

9 DPI-SSL クライアント検査を有効にする各ゾーンに対して ステップ 6 から ステップ 8 を繰り返します。

ゾーン上で DPI-SSL サーバを有効にするには:

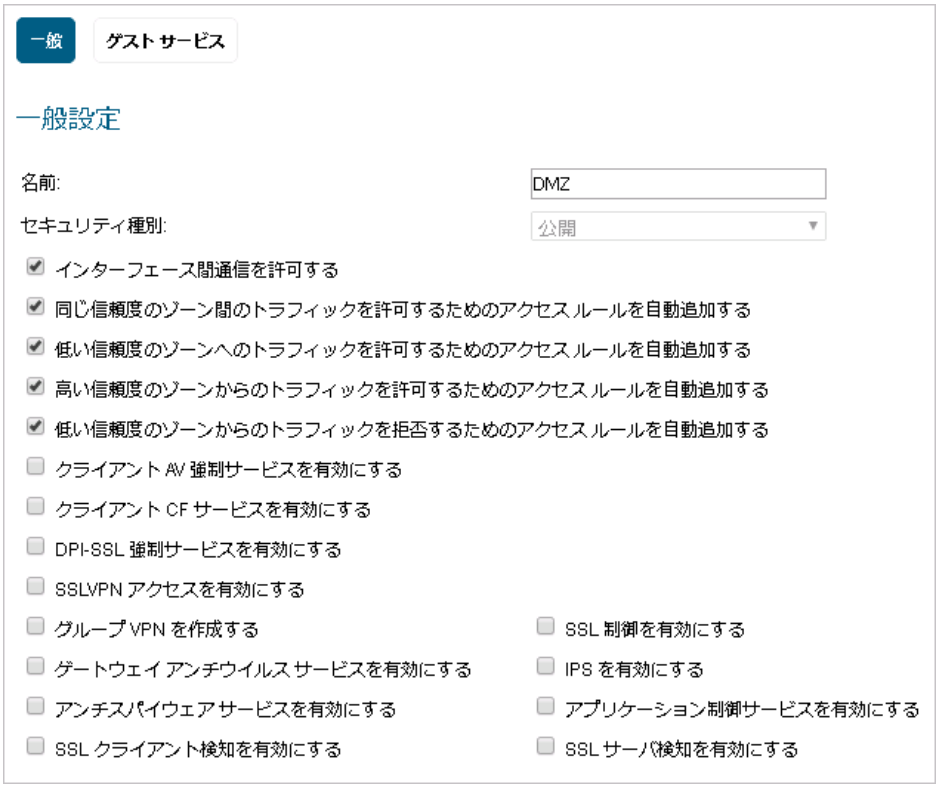
1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS サーバ**」に移動します。

2 「**SSL サーバ検査を有効にする**」を選択します。このオプションは既定では選択されていません。

3 「**適用**」を選択して DPI-SSL/TLS サーバの設定を終了します。

4 「**管理 | システム設定 > ネットワーク > ゾーン**」に移動します。

5 設定するゾーンの「**編集**」アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。



6 「**SSL サーバ検知を有効にする**」を選択します。このオプションは既定では選択されていません。

7 「**OK**」を選択してゾーンの設定を終了します。

8 DPI-SSL サーバ検査を有効にする各ゾーンに対して ステップ 5 から ステップ 7 を繰り返します。

アクセス ルールに基づいた DPI-SSL 制御

DPI-SSL がクライアントとサーバの両方に対してアクセス ルールによって制御可能になりました。

DPI-SSL クライアントおよび/またはサーバをアクセス ルールによって制御するには:

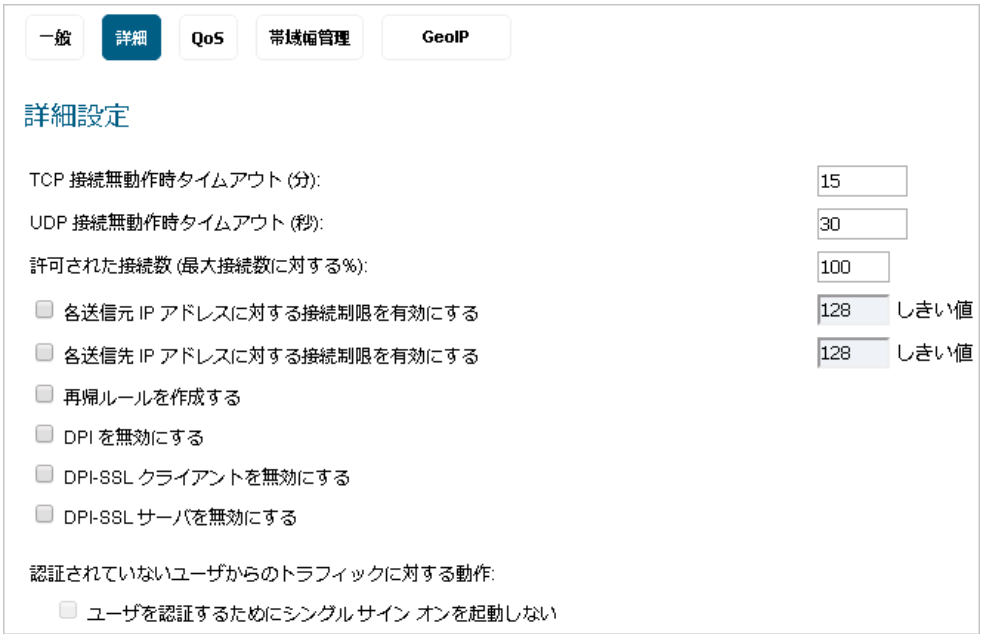
1 「**管理 |ポリシー > ルール > アクセス ルール**」に移動します。

2 どちらかを実行します:

- 「**追加**」を選択してアクセス ルールを追加します。
- 既存のアクセス ルールの「**編集**」アイコンを選択します。

「**ルールの追加**」ダイアログが表示されます。

3 「**詳細**」を選択します。



4 このアクセス ルールに対して DPI-SSL クライアントを無効にするには「**DPI-SSL クライアントを無効にする**」を選択します。このオプションは既定では選択されていません。

5 このアクセス ルールに対して DPI-SSL サーバを無効にするには「**DPI-SSL サーバを無効にする**」を選択します。このオプションは既定では選択されていません。

6 アクセス ルールの設定を完了します。

7 「**OK**」を選択します。

TLS 証明書ステータス要求の拡張

DPI-SSL は、新しい TLS 証明書ステータス要求拡張 (正式には OCSP ステープル) をサポートするようになりました。この拡張をサポートすることにより、すでに確立されたチャンネルを通じて DPI-SSL クライアントに証明書のステータス情報が配信されるため、オーバーヘッドが削減され、パフォーマンスが向上します。

この機能の詳細については、*SonicWall SonicOS 6.5 システム セットアップ*を参照するか、テクニカル サポートにお問い合わせください。

ローカル CRL のサポート

証明書失効リスト (CRL) は、発行した認証局 (CA) によって予定された有効期限前に失効され、もはや信頼されるべきではないデジタル証明書のリストです。このリストの CA に連絡する際の問題は、ブラウザが CA のサーバーに到達したかどうか、または攻撃者が失効チェックをバイパスするために接続を傍受したかどうかをブラウザが確認できないことです。

ローカル CRL は、標準 CRL (またはオンライン CRL) と関連しています。一般的な CRL の場合、クライアントは CRL 配布ポイントから CRL をダウンロードする必要があります。クライアントが CRL をダウンロードできない場合、クライアントは既定では証明書を信頼します。 通常の CRL とは異なり、ローカル CRL は、証明書が失効しているかどうかを確認するために、DPI-SSL のインポート メモリにローカルで失効した証明書のリストを保持します。

この機能の詳細については、*SonicWall SonicOS 6.5 システム セットアップ*を参照するか、テクニカル サポートにお問い合わせください。

強化された DPI-SSL 証明書検証

認証局 (CA) には、ルート CA と中間 CA の2種類があります。SSL 証明書を信頼するには、接続しているデバイスの信頼できるストアに含まれている CA によって証明書が発行されている必要があります。ルート証明書からエンドユーザー証明書までの SSL 証明書のリストは、SSL 証明書チェーンを表します。

この機能により、中間証明書が DPI-SSL によって保存された信頼されたルート CA にない場合に、DPI-SSL が証明書チェーンを検証できます。証明書チェーンを検証することは、特定の証明書チェーンが正しい形式で、有効で、正しく署名され、信頼できることを保証するプロセスです。

ECDSA 系暗号のサポート

以前は、DPI-SSL クライアントは TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 のような RSA 系暗号だけをサポートしていました。DPI-SSL クライアントは、ECDSA (Elliptic Curve Digital Signature Algorithm) 暗号をサポートするようになりました:

- TLS_ECDHE_ECDSA_WIATH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

DPI-SSL と CFS HTTPS コンテンツ フィルタの独立稼働

以前は、DPI-SSL と CFS HTTPS コンテンツ フィルタは相互に排他的であり、同時に有効にすることができませんでした。これら両方の機能を同時に有効にして、次のように機能させることができるようになりました:

- DPI-SSL クライアント検査が無効の場合、コンテンツ フィルタ サービスが HTTPS 接続をフィルタします。
- DPI-SSL クライアント検査が有効で、コンテンツ フィルタ オプションが選択されていない場合、コンテンツ フィルタ サービスが HTTPS 接続をフィルタします。
- DPI-SSL クライアント検査が有効で、コンテンツ フィルタ オプションが選択されている場合、CFS は HTTPS 接続をフィルタしません。

SSH X11 転送の遮断

X は、Unix ワークステーションにとって一般的なウィンドウ システムです。 X を使用して、ユーザはリモート X アプリケーションをユーザのローカル ディスプレイ上のウィンドウで開いて実行 (逆にリモート ディスプレイ上でローカル アプリケーションを実行) することができます。リモート サーバがファイアウォールの外側にあり、管理者がリモート接続を遮断している場合でも、ユーザーは SSH トンネリングを使用してローカル マシン上に X ディスプレイを取得できます。したがって、ユーザはファイアウォール上のアプリケーション ベースのセキュリティ ポリシーを迂回することができ、セキュリティ リスクが発生します。

アプリケーションと X サーバ間の X プロトコル セッションは、ネットワーク上で送信されている間に暗号化されないため、セキュリティと強力な認証を提供するために、SSH 接続を通して X11 プロトコル接続をルートできます。この機能は X11 転送と呼ばれます。

SSH クライアントは、SSH サーバに接続するときに X 転送を要求します (クライアントで X 転送が有効と仮定します)。サーバがこの接続で X 転送を許可している場合、通常はログインが進行しますが、この裏でサーバは特別な手順を実行します。ターミナル セッションを処理するだけでなく、サーバはリモート マシン上で実行されているプロキシ X サーバーとして自身を設定し、リモート シェルの DISPLAY 環境変数をプロキシの X 表示を指すように設定します。X クライアント プログラムが実行されている場合は、プロキシに接続します。プロキシは実際の X サーバと同様に振る舞い、ローカル マシン上の X サーバに接続してプロキシ X クライアントとして動作するよう SSH クライアントに指示します。SSH クライアントとサーバは協力して、2 つの X セッション間で SSH パイプを介して X プロト

コル情報をやりとりし、X クライアント プログラムはまるでディスプレイに直接接続されているかのように画面に表示されます。

DPI-SSH X11 転送は、次のクライアントをサポートします:

- Cygwin の SSH クライアント
- Putty
- secureCRT
- Ubutu の SSH
- CentOS の SSH

DPI-SSH X11 転送は、次の OS 上の SSH サーバをサポートします:

- Fedora
- Ubuntu

SSH X11 転送は、ルート モードおよびワイヤ モードの両方を次のようにサポートします:

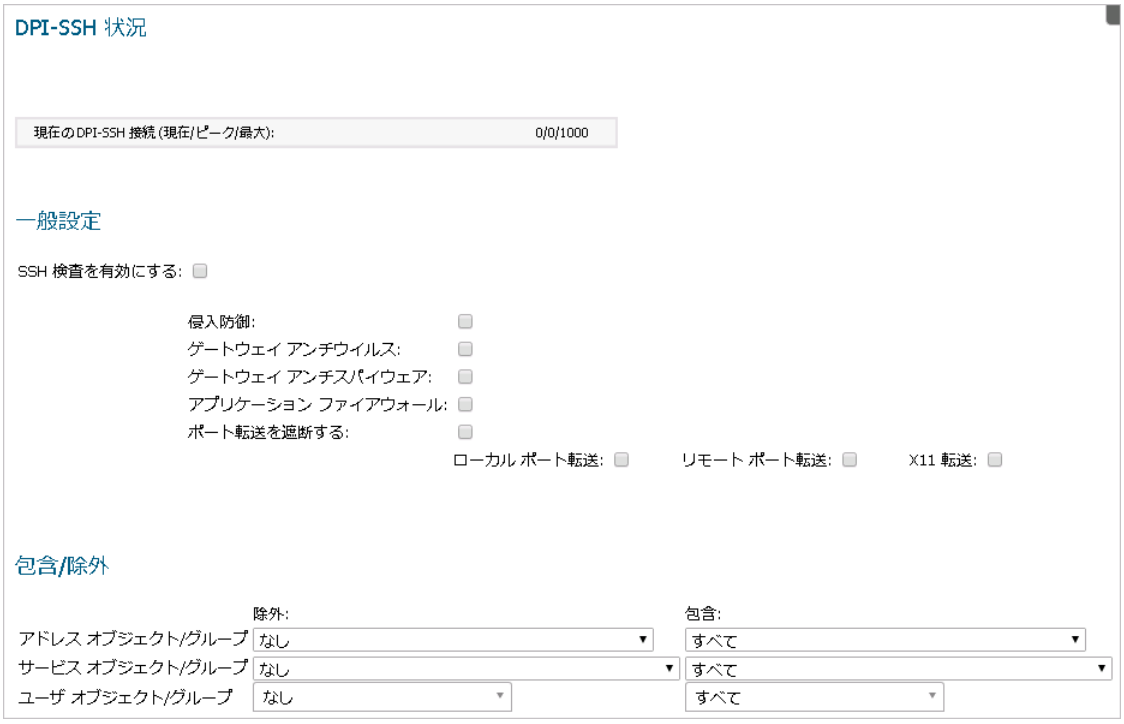
- ワイヤ モードでは、SSH X11 転送は保護された (インライン トラフィックのアクティブ DPI) モードでのみサポートされます。
- ルート モードでは制限がありません。

SSH X11 転送でサポートされる最大接続数は、DPI-SSH と同じ 1000 です。

DPI-SSH X11 転送には、有効な SonicWall DPI-SSH ライセンスが必要です。

SSH X11 転送を遮断するには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」に移動します。



2 「**X11 転送**」を選択します。

3 「**適用**」を選択します。

復号化されたパケットの元のポート番号の保持

暗号化された接続の DPI-SSL / DPI-SSH 接続に対して、復号化されたパケットは宛先ポートを 80 (HTTPS の場合) と表示します。復号化されたパケットがパケット キャプチャ/ Wireshark で監視された場合に、元のポート番号が保持されるようになりました。ポート番号の変更は、パケット キャプチャのみに適用され、実際のパケットまたは接続キャッシュには適用されません。

SonicWave 機能

トピック:

- 保護された管理フレーム (IEEE 802.11w)
- SonicWave の RRM および WNM サポート (IEEE 802.11k および IEEE 802.11v)
- SonicWave の保護された高速ローミング (IEEE 802.11r)
- KRACK 検出と防御
- 高度な LTE モデムのサポート
- ファームウェア管理サポート
- 複数モデム間の負荷分散
- RSSI しきい値サポート
- RADIUS サーバ認証キャッシュ

保護された管理フレーム (IEEE 802.11w)

WLAN は、すべての無線デバイスが同じ無線メディアを共有するため、攻撃に対して脆弱です。攻撃者は無線フレームを簡単に監視し、偽装することができます。このセキュリティ問題を解決するため、IEEE は認証と暗号化の方法として WEP を開発しましたが、現在は認証に 802.1X、暗号化に CCMP を使用する 802.11i に置き換えられました。

フレームが暗号化されている場合でも、攻撃者はフレームをキャプチャできますが、フレームを復号化して初期データを取得することはできません。ただし、802.11i はデータフレームのみを保護できます。無線クライアントは、認証、非認証、参加、不参加、ビーコン、プローブなどの管理フレームを使用して、ネットワーク サービスのセッションを開始および切断します。あるレベルの機密性を提供するために暗号化できるデータ トラフィックとは異なり、これらのフレームはすべてのクライアントによって認知し理解される必要があるため、オープンまたは暗号化されていない状態で送信される必要があります。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造から保護する必要があります。たとえば、攻撃者がクライアントの MAC アドレスを取得した場合、AP の名前でクライアントに不参加要求を送信したり、クライアントの名前で AP に再参加要求を送信したりすることができます。クライアントはどちらの状況でもログオフされます。

IEEE 802.11w-2009 は、無線管理フレームを保護するために IEEE 802.11 標準で承認された改正です。これは、Protected Management Frames (PMF) 標準とも呼ばれます。802.11w プロトコルは、Protected Management Frames (PMF) サービスで保護された一連の堅牢な管理フレームにのみ適用されます。これには、不参加、非認証、堅牢アクション フレームが含まれます。802.11w は特定の管理フレームだけを保護し、AP とクライアント間の通信には影響しません。802.11w は、AP とクライアントの両方で 802.11w が有効な場合にのみ有効です。

802.11w には次の利点があります:

機密性

ユニキャスト管理フレームの暗号化:

- データフレームと同じ PTK を使用

- 追加の認証データ (AAD) を使用して以前に暗号化されていないフレームヘッダを保護
- ユニキャスト管理フレームを処理する拡張 AES-CCM
- 再生保護のための分離受信シーケンス カウンタ (RSC)

グループ アドレス指定フレーム保護

Broadcast / Multicast Integrity Protocol (BIP) は、ブロードキャストとマルチキャストの整合性を保護し、再生攻撃を防ぎ、クライアントがブロードキャスト/マルチキャスト攻撃を詐称するのを防ぎます。ブロードキャスト/マルチキャスト管理フレームに対して:

- WPA 鍵ハンドシェイク中に受け取った新しい Integrity Group Temporal Key (IGTK) を使用
- 新しいアルゴリズム: Broadcast Integrity Protocol (BIP)
- 新しい情報要素: シーケンス番号 + 暗号化ハッシュによる管理 MIC IE (AES128-CMAC ベース)

接続保護

セキュリティ アソシエーション (SA) クエリは、再参加要求をスプーフィングすることによって、クライアントがオフラインになるのを防ぐことができます。

802.11w は特定の管理フレームだけを保護し、AP とクライアント間の通信には影響しません。これは AP とクライアントの両方で 802.11w が有効な場合にのみ有効です。

802.11w の保護された管理フレームを有効にするには:

1 「**管理 | 接続 > アクセス ポイント > 基本設定**」に移動します。

2 「**SonicPoint/SonicWave プロビジョニング**」テーブルまでスクロールします。

3 SonicWave の「**設定**」アイコンを選択します。「**SonicWave プロファイルの編集 - SonicWave**」ダイアログが表示されます。

4 「**5GHz 無線基本**」を選択します。

5 「**無線セキュリティ**」までスクロールします。

6 「**認証種別**」に対して WPA 関連の認証種別を選択します。

重要 : 保護された管理フレームを機能させるためには、認証種別を WPA 関連の認証種別にする必要があります。

7 「**PMF オプション**」から、以下のどちらかを選択します:

- **有効** - サービスはクライアントに対して任意です。
- **必須** - クライアントは AP に接続する前にサービスを有効にする必要があります。

8 「**2.4GHz 無線基本**」を選択します。

9 ステップ 5 から ステップ 7 を繰り返します。

10 「**OK**」を選択します。

SonicWave の RRM および WNM サポート (IEEE 802.11k および IEEE 802.11v)

無線 LAN (WLAN) 無線の測定により、ステーションは、無線リンクのパフォーマンスや無線環境での観測やデータ収集を通じて、ステーションが存在する無線環境を理解することができます。ステーションは、ローカルで測定を行うか、別のステーションから測定を要求するか、または 1 つ以上の測定を行い結果を返すように別のステーションによって要求されることがあります。無線測定データは、ステーション管理および上位プロトコル レイヤで利用でき、さまざまなアプリケーションに使用できます。この測定により、ステーションの動作を無線環境により良く適合させることが可能になります。無線測定サービスには、ベンダ間で標準的な測定値を提供することにより、WLAN の機能、信頼性、および保守性を拡張する測定が含まれており、サービスにより測定結果データが通信スタックの上位層に提供されます。

標準測定の実行と、測定情報を上位層に配信することに加え、必要なパフォーマンス レベルを達成するために定量化可能な無線環境測定を必要とする VoIP、ビデオ オーバー IP、ロケーション ベースのアプリケーションなどのアプリケーションもあります。

VoIP やビデオ ストリーミングなどの技術のモビリティ要件に対応するために、チャンネル ロード要求/レポートや 近隣者要求/レポートなどの 無線測定を使用して遷移情報を収集することができ、同じ ESS 内の BSS 間のハンドオフを大幅に高速化できます。ステーション (AP または非 AP ステーションのいずれか) は、この情報にアクセスして使用することにより、利用可能なスペクトル、電力、および帯域幅を通信に使用する最も効果的な方法について、妥当な決定を行うことができます。

IEEE 802.11 無線ネットワーク管理 (改正 8) は、無線ネットワークに接続されている間にクライアント デバイスの構成を可能にする IEEE 802.11 標準の改正である。WNM (無線ネットワーク管理) をサポートするステーションは、無線ネットワークのパフォーマンスを向上させるために、相互 (アクセスポイントと無線クライアント) に情報を交換できます。 802.11v を使用すると、クライアント デバイスは、RF 環境に関する情報を含むネットワーク トポロジに関する情報を交換し、各クライアント ネットワークに認識させ、無線ネットワークの全体的な改善を容易にすることができます。

ステーションは WNM プロトコルを使用して運用データを交換し、各ステーションがネットワーク状態を認識し、ステーションがネットワークのトポロジーと状態をよりよく認識できるようにします。WNM プロトコルは、ステーションが配置された干渉の存在を認識し、ステーションがネットワーク状況に基づいて RF パラメータを管理できるようにする手段を提供します。

WNM はネットワーク状況に関する情報を提供するだけでなく、位置情報を交換する手段を提供し、同じ無線インフラストラクチャ上で複数の BSSID 機能サポートを提供し、グループ アドレス指定フレームの効率的な配信をサポートし、AP からフレームを受信せずにステーションが長時間休止可能な WNM 休止モードを有効にします。

近隣者レポート要求は、クライアントから AP に送信されます。APは、(クライアントがそうすることを選択した場合) クライアントとの再参加を行う既知の候補である近隣 AP に関する情報を含む近隣者

レポートを返します。これにより近隣者レポート要求/報告ペアは、クライアントが現在関連付けられている AP の近隣 AP に関する情報を収集することを可能にし、この情報は、ローミング中の新しい接続ポイントの潜在的候補の識別として使用することができます。

近隣者レポート要求/報告の利点は次のとおりです:

- **スキャンの高速化** - 時間のかかるスキャン作業 (AP を積極的にプロービングするかビーコンのすべてのチャンネルを受動的にリッスンするか) の代わりに、クライアントは既知の使用可能な近隣者にリストを絞り込むことができます。これは、クライアントが複数の WLAN をリッスンできる高密度環境で特に役立ちます。
- **クライアントの消費電力削減** - スキャン (特にアクティブスキャン) にかかる時間も、クライアントのバッテリ電力を消費します。近隣者レポートがローミング前に情報を提供するため、消費電力が少なくなる可能性があります。
- **WLAN エア タイムの効率的な使用** - アクティブなスキャンは、クライアント リソース (CPU、メモリ、無線など) の観点からも時間がかかるだけでなく、エア タイムを消費します。たとえば、近隣者が認識していないクライアントは、いわゆるワイルドカード プローブ要求に従事する可能性があります (一部のクライアントはこれらを破棄します)。このシナリオでは、通常、プローブ要求を聞くすべての AP がプローブ応答を生成します。言い換えれば、1 台のクライアントに対して N 個の AP が N 個のプローブ応答を生成します。複数のクライアントがワイルドカード プロービングに頼っている場合、クライアントが近隣者リクエストを使用していないため、RF 環境が管理トラフィックですぐに汚染される可能性があります。これは WLAN 全体に対して悪影響があります。

SonicPoint は BSS の最大アイドル期間管理をサポートしています。SonicWave は、無線ネットワークのパフォーマンスを向上させるために、さらに 2 つの WNM サービスをサポートしています。

- **BSS 移行管理** - ネットワーク負荷分散または BSS 終了のために、AP がボイス クライアントに特定の AP に移行するように要求するか、またはボイス クライアントに一連の優先 AP を提案できます。これは、ボイス クライアントがローミングするときに、自身が移行すべき最善の AP を識別するために役立ちます。

  BSS 移行機能により、個々の音声トラフィック負荷を ESS 内のより適切な参加ポイントに (移行を介して) シフトすることによって、ネットワーク内の音声クライアントのスループット、データ レートおよび QoS を向上させることができます。

  802.11v BSS 移行管理要求は、クライアントに与えられた提案です。クライアントは、提案に従うかどうかを自身で判断できます。

  フレーム種別 - BSS 移行管理は、次のフレーム種別を使用します:

  - **クエリ** - 関連付けられた AP が BSS 移行機能をサポートしていることを示す場合、クエリ フレームが BSS 移行候補リストを関連する AP に要求する BSS 移行管理をサポートする音声クライアントによって送信されます。
  - **要求** - BSS 移行管理をサポートする AP は、BSS 移行管理クエリ フレームに対して BSS 移行管理要求フレームで応答します。AP は、クライアントが BSS 移行管理機能をサポートしている場合はいつでも、求められていない BSS 移行管理要求フレームを音声クライアントに送信することもできます。この要求フレームには、不参加フラグも含まれています。フラグが設定されている場合、AP は指定された間隔の後にクライアントを強制的に不参加にします。
  - **応答** - 応答フレームは、音声クライアントによって AP に返送され、移行を受け入れるか拒否するかを通知します。

  802.11k および 802.11v クライアント - 802.11k 対応クライアントの場合、クライアント管理フレームワークは、AP によって送信されたビーコン レポート要求に応答して、クライアントによって生成された実際のビーコン レポートを使用します。このビーコン レポートは、そのクライアントの仮想ビーコン レポートを置き換えます。802.11v 対応クライアントの場合、コン

トローラは 802.11v BSS 移行メッセージを使用して、AP からクライアント誘導トリガを受信すると、クライアントを目的の AP に誘導します。

- **WNM 休止モード** - 非アクセス ポイント (非 AP) ステーション (STA) のための拡張省電力モードで、非 AP STA がすべての配信トラフィック指示メッセージ (DTIM) ビーコンフレームをリッスンする必要がなく、グループの一時的キー/整合性グループの一時的キー (GTK / IGTK) 更新を実行しません。

  WNM 休止モードにより、非 AP STA は指定された時間休止する AP に信号を送信できます。これにより、非 AP STA は電力消費を低減し、非 AP STA に AP との間で送受信するトラフィックがない間も関連付けを維持することができます。

重要 : WNM 休止モードが有効で、ステーションが WNM 休止モードをサポートしている場合は、鍵再インストール攻撃を回避するようにステーションを更新してください。

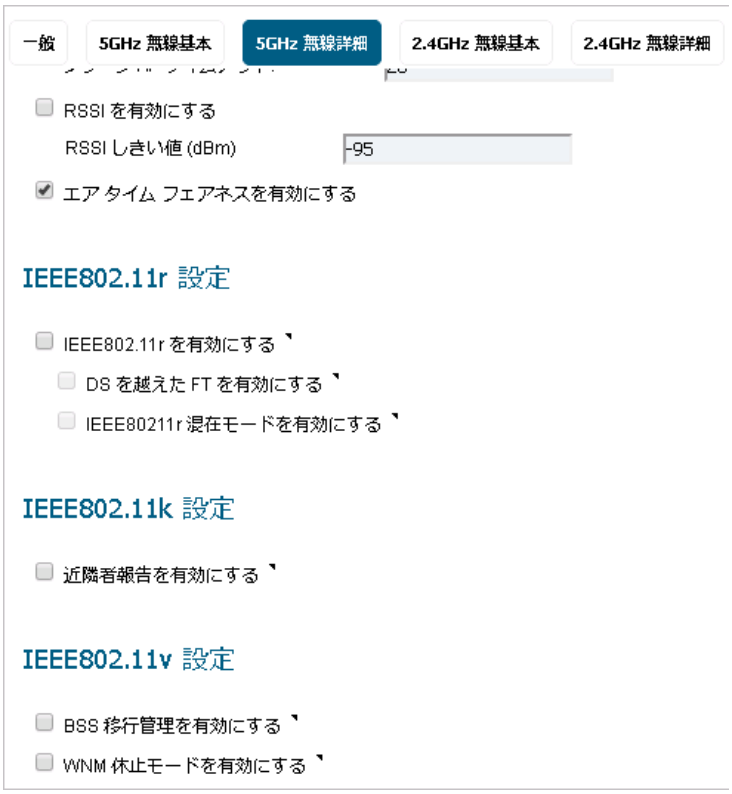
SonicWave プロビジョニング プロファイル内で RRM と WNM サポートを有効にするには:

1 「**管理 | 接続 > アクセス ポイント > 基本設定**」に移動します。

2 「**SonicPoint/SonicWave プロビジョニング**」テーブルまでスクロールします。

3 SonicWave の「**設定**」アイコンを選択します。「**SonicWave プロファイルの編集 - SonicWave**」ダイアログが表示されます。

4 「**5GHz 無線詳細**」を選択します。



5 「**IEEE802.11k 設定**」までスクロールします。

6 近隣者報告を有効にするには、「**近隣者報告を有効にする**」を選択します。このオプションは既定では選択されていません。

7 「**IEEE802.11v 設定**」までスクロールします。

8 BSS 移行管理を有効にするには、「**BSS 移行管理を有効にする**」を選択します。このオプションは既定では選択されていません。

9 WNM 休止モードを有効にするには、「**WNM 休止モードを有効にする**」を選択します。このオプションは既定では選択されていません。

10 「**2.4GHz 無線詳細**」を選択します。

11 ステップ 5 から ステップ 9 を繰り返します。

12 「**OK**」を選択します。

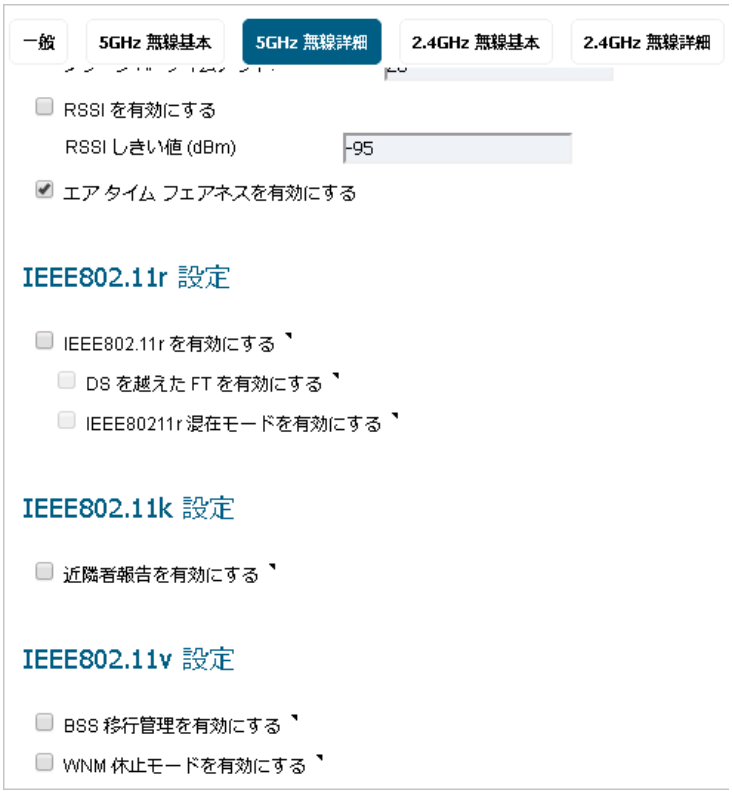
SonicWave VAP プロファイル内で RRM と WNM サポートを有効にするには:

1 「**管理 | 接続 > アクセス ポイント > 仮想アクセス ポイント**」に移動します。

2 「**仮想アクセス ポイント プロファイル**」テーブルまでスクロールします。

3 プロファイルの「**設定**」アイコンを選択します。「**仮想アクセス ポイント プロファイルを追加または編集する**」ダイアログが表示されます。

4 「**IEEE802.11k 設定**」までスクロールします。



5 近隣者報告を有効にするには、「**近隣者報告を有効にする**」を選択します。このオプションは既定では選択されていません。

6 「**IEEE802.11v 設定**」までスクロールします。

7 BSS 移行管理を有効にするには、「**BSS 移行管理を有効にする**」を選択します。このオプションは既定では選択されていません。

8 WNM 休止モードを有効にするには、「**WNM 休止モードを有効にする**」を選択します。このオプションは既定では選択されていません。

9 「**OK**」を選択します

SonicWave の保護された高速ローミング (IEEE 802.11r)

一般に Wi-Fi と呼ばれる IEEE802.11 は、無線通信に対して広く使用されています。導入された実装の多くは数百メートルの有効範囲しか持たないため、通信を維持するために、移動中のデバイスはあるアクセス ポイントから別のアクセス ポイントにハンドオフする必要があります。自動車ではこれが起こりやすく、5 秒から 10 秒ごとにハンドオフすることもあります。

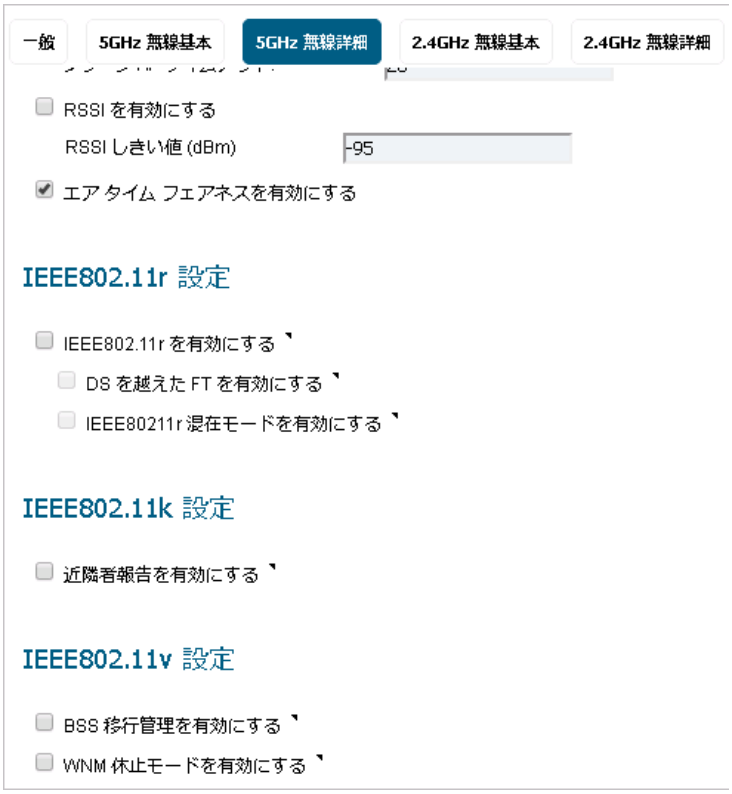
ハンドオフは既存の標準で既にサポートされています。ハンドオフのための基本的なアーキテクチャは、802.11r の有無にかかわらず 802.11 と同一で、モバイル デバイスには、いつハンドオフするのか、どのアクセス ポイントにハンドオフしたいのかをすべて決定する役割があります。802.11 の初期段階では、ハンドオフはモバイル デバイスにとってずっと簡単な作業でした。デバイスが新しいアクセス ポイントとの接続を確立するために 4 つのメッセージしか必要としませんでした (クライアントが古いアクセス ポイントに送信できるオプションの "I'm leaving" メッセージ [非認証と不参加パケット] を数えると 5 つです)。 ただし、802.1x 認証を使用する 802.11i や、アドミッション制御要求を使用する 802.11e や WMM など、標準に追加機能が増えたため、必要なメッセージ数が大幅に増加しました。これらの追加メッセージが交換されている間は、音声通話を含めモバイル デバイスのトラフィックは処理できず、ユーザに対する損失は数秒に達する可能性があります。 一般的に、エッジ ネットワークが音声通話で考慮する必要がある遅延または損失の最大量は 50 ミリ秒です。

802.11r は、セキュリティとサービス品質がハンドオフ プロセスに追加され、それを元の 4 メッセージ交換に復元するという追加の負担を取り消します。このようにして、ハンドオフの問題は解消されませんが、少なくとも現状に戻されます。

802.11r 標準のために現在想定されている主なアプリケーションは、標準の携帯電話ネットワークの代わりに (またはそれに加えて) 無線インターネット ネットワークで動作するように設計された携帯電話による VoIP (Voice over IP) です。

高速移行 (IEEE 802.11r) を設定するには:

1. 「**管理 | 接続 > アクセス ポイント > 基本設定**」に移動します。
2. 「**SonicPoint/SonicWave プロビジョニング**」テーブルまでスクロールします。
3. SonicWave の「**設定**」アイコンを選択します。「**SonicWave プロファイルの編集 - SonicWave**」ダイアログが表示されます。
4. 「**5GHz 無線詳細**」を選択します。
5. 「**IEEE802.11r 設定**」までスクロールします。



6 高速移行を有効にするには、「**IEEE802.11r を有効にする**」を選択します。このオプションは既定では選択されていません。有効にすると、続く2 つのオプションが利用可能になります。

7 DS を越えた高速移行を有効にするには、「**DS を越えた FT を有効にする**」を選択します。このオプションは既定では選択されていません。

8 混在モードで高速移行を有効にするには、「**IEEE80211r 混在モードを有効にする**」を選択します。このオプションは既定では選択されていません。

9 「**2.4GHz 無線詳細**」を選択します。

10 ステップ 5 から ステップ 8 を繰り返します。

11 「**OK**」を選択します。

KRACK 検出と防御

セキュリティ研究者である Mathy Vanhoef 氏は、最新の Wi-Fi ネットワークを保護するために使用されているセキュリティ プロトコルである WPA2 を解読し、攻撃者が鍵再インストール攻撃 (KRACK) と Vanhoef 氏のテクニックを用いて以前に安全に暗号化されたと思われる情報を読み取り、クレジットカード番号、パスワード、チャットメッセージ、電子メール、写真などの機密情報を盗み出すことができることがわかりました。

SonicWave は現在、KRACK 中間者 (MitM) アクセス ポイントを検出して防御し、「**調査 | ログ > イベント ログ**」ページに攻撃を記録して、影響を受けたパケットを「**管理 |接続 > アクセス ポイント> 高度な IDP**」ページの「**KRACK スニファ パケット**」セクションに表示します。

KRACKの 検出と防御が有効になっている場合、SonicWave は無線環境を定期的にスキャンし、KRCAK MITM AP と MITM と対話するクライアントを探します。以下のいずれかが発生すると、メッセージが「**調査 | ログ > イベント ログ**」ページに報告されます。

- MITM AP
- クライアントと MITM AP の通信

- MITM AP からのクライアントの不参加

KRACK 検出と防御を有効にするには:

1 「**管理 |接続 > アクセス ポイント> 高度な IDP**」に移動します。

2 「**KRACK MITM AP からクライアントの関連付けを解除する**」を有効にします。

3 「**適用**」を選択します。

高度な LTE モデムのサポート

PPP は従来の 3G USB モデムで広く使用されており、セルラー モバイル ネットワークへの直接接続を確立していますが、PPP はもはや高速接続には適していません。LTE USB モデムは、ホスト オペレーティング システム (OS) に対してイーサネット インターフェースを直接 IP アドレスで提供するため、ホスト OS は標準の IP プロトコルを使用して USB 内部ウェブ サーバにアクセスし、動的 IP アドレスを取得、USB モデムを管理し、 高速 LTE ネットワークへの接続を確立して、デバイスの状態およびデータ使用状況を監視することができます。SonicOS は、低速 3G USB モデムで動作する PPP とダイレクト イーサネット IP インターフェースをサポートする LTE USB モデムの両方をサポートします。

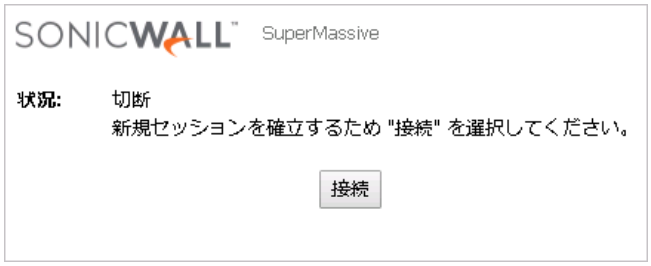
PC 上で LTE モデムを使用する場合、ユーザーはデバイスを接続し、Windows はデバイス用の RNDIS (Remote Network Driver Interface Specification) インターフェースを確立します。このデバイスは ISP と自動的に接続し、手作業を挟むことなく数秒でホストにインターネット アクセスを提供できます。SonicOS は、Hi-Link モデムのこの使い易さと、従来のモデムとの互換性を維持します。

LTE USB モデムが SonicWall セキュリティ装置に接続されると、SonicOS はそのモデルを検出し、「**管理 | システム設定 > ネットワーク > インターフェース**」ページに U0 インターフェースを表示します。 このインターフェースは、既定で WAN ゾーンに属していて、フェイルオーバーおよび負荷分散に使用できて、また LTE 接続、プロファイル、詳細設定の構成にも使用できます。

非 PPP 接続プロファイルを「**3G/4G/LTE 設定**」ダイアログ (**管理 | 接続 > 3G/4G/LTE > 接続プロファイル**) で設定するときに、「**優先ネットワーク技術**」オプションが 「**接続種別**」、「**ダイアル番号**」、「**ユーザ名**」、および「**ユーザ パスワード**」オプションの代わりになります。

LTE モデムが検出されると、それは 「**監視 | 現在の状況 > 3G/4G/LTE 状況**」に表示されます。 このページでモデムの設定を行います。

モデムを使用するには、「**接続マネージャ**」の「**接続**」ボタンを選択して、USB デバイスをネットワークに接続する必要があります。



状況が「**接続中**」に変わります。

WAN インターフェースのアドレスと DNS アドレスは、ISP の DHCP サーバによって割り当てられます。セキュリティ装置は、このDHCP IP アドレスを U0 インターフェースの IP アドレスに使用します。

モデムを切断するには、「**切断**」ボタンを選択します。

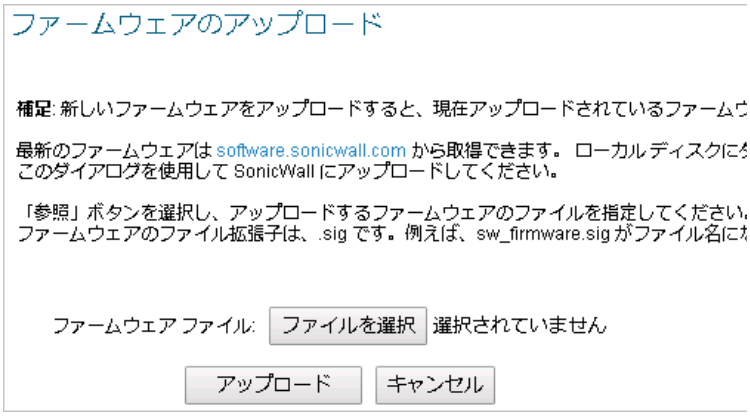
ファームウェア管理サポート

管理インターフェースに新しいページ、「**管理 | 接続性 > アクセス ポイント > ファームウェア管理**」が追加されました。このページでは、セキュリティ装置で使用される SonicWave / SonicPoint イメージの格納を管理し、アップロードするローカル ファイルを選択することができます。

ファームウェアを手動でアップロードするには:

1 「**管理 | 接続性 > アクセス ポイント > ファームウェア管理**」に移動します。

2 ファームウェアをアップロードする SonicWave/SonicPoint の「**編集**」アイコンを選択します。「**ファームウェアのアップロード**」ダイアログが表示されます。



3 「**ファイルを選択**」を選択します。「**ファイルのアップロード**」ダイアログが表示されます。

4 ファイルを選択します。

5 「**開く**」を選択します。

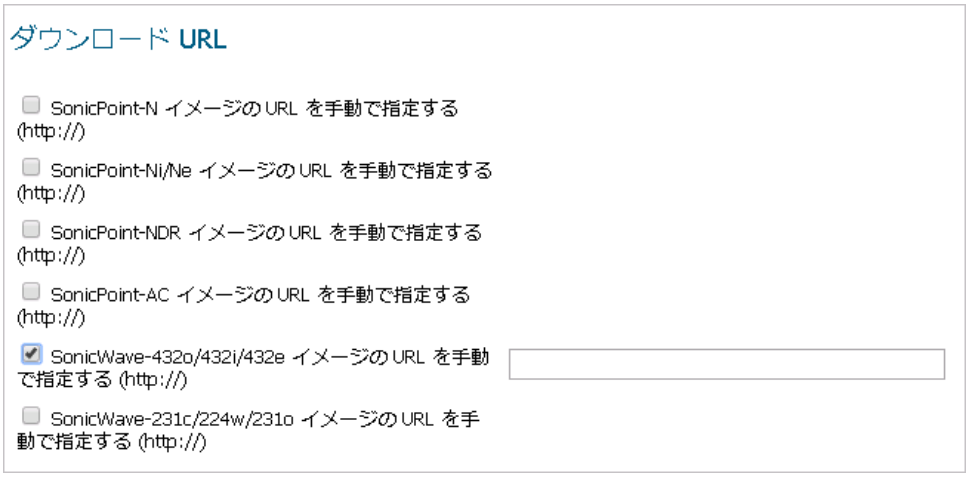
6 「**アップロード**」を選択します。

イメージの URL を指定するには:

1 「**管理 | 接続性 > アクセス ポイント > ファームウェア管理**」に移動します。

2 「**ダウンロード URL**」までスクロールします。

3 ダウンロード URL を指定するイメージを選択します。 フィールドが使用可能になります。



4 フィールドにイメージの場所を示す URL を入力します。

5 「**適用**」を選択します。

複数モデム間の負荷分散

複数の SonicPoint / SonicWave と複数の 3G / 4G モデム (それぞれ 2 つ以上) が利用可能な場合、これら複数の SonicPoint / SonicWave とモデムの間で負荷分散を実行できます。

複数の 3G / 4G モデムを使った負荷分散を構成するには:

1 手動または 3G / 4G / LTE ウィザードを使用して、SonicWave / SonicPoint および 3G / 4G モデムの各ペアに固有の VLAN を割り当てます。

2 「**管理 |システム セットアップ > ネットワーク > フェイルオーバーと負荷分散**」に移動して、これらの VLAN インターフェースを LB グループに追加します。 詳細については『*SonicWALL SonicOS 6.5 システム設定*』管理マニュアルを参照してください。

RSSI しきい値サポート

エリア全体で良好な Wi-Fi カバレッジを提供するために複数のアクセス ポイントが必要なほど広いエリアがあります。 ほとんどの人は、Wi-Fi クライアント (ラップトップまたはタブレット) が最も近いアクセス ポイントを検出して移動することを期待しています。残念なことに、多くの Wi-Fi クライアントでは、このような動作が期待できません。代わりに、それらにとって一般的にはより良い選択となる近くのアクセス ポイントに移動するよりも、元の参加したアクセス ポイントに留まる傾向があります。この動作は、スティッキー動作と呼ばれ、RSSI (Received Signal Strength Indicator) が低く、SNR (Signal-to-Noise Ratio) が高くなります。元のアクセスポイントから離れてクライアントが移動すると、RSSI は弱くなり、SNR は悪化し、再送信が発生し、動的なレートシフトが発生し、クライアントははるかに低いデータレートで通信することになります。より低いデータレートは、同一の情報を転送するために多くのエアタイムを消費し、その結果、チャンネル利用率が高くなります。 理想的には、クライアントは最も近いアクセス ポイントにローミングし、その結果として得られる RF スペースは誰にとっても良いでしょう。SonicOS は最適化されたローミングの問題を解決します。クライアントが特定の RSSI、データレート、またはその両方に達すると、アクセス ポイントからクライアントの参加が解除され、クライアントはより近いアクセスポイントに参加します。 RSSI は、アクセス ポイントの観点からのものです。 RSSI とデータレートの両方を設定可能です。

RSSI 測定は、デバイス上の受信信号の相対的品質を示します。RSSI は、アンテナおよびケーブル レベルで損失が発生した後に受信される電力レベルを示します。RSSI 値が高いほど信号が強くなります。負の数で測定された場合、ゼロに近い数値は通常、より良い信号を意味します。一例として、-50 はかなり良い信号、-75 はそこそこ妥当、-100 は全く信号がありません。

RSSI とdBm は異なる測定単位ですが、両方とも信号強度を示します。dBm は、1 mW (ミリワット) を基準とした測定電力の電力比です。dBm は絶対指数ですが、RSSI は相対指数です。

意味のある良質の信号測定のために、信号電力からライン上のノイズを減らします。信号とノイズの差が大きいことは、WiFi 信号強度が良いことを意味します。

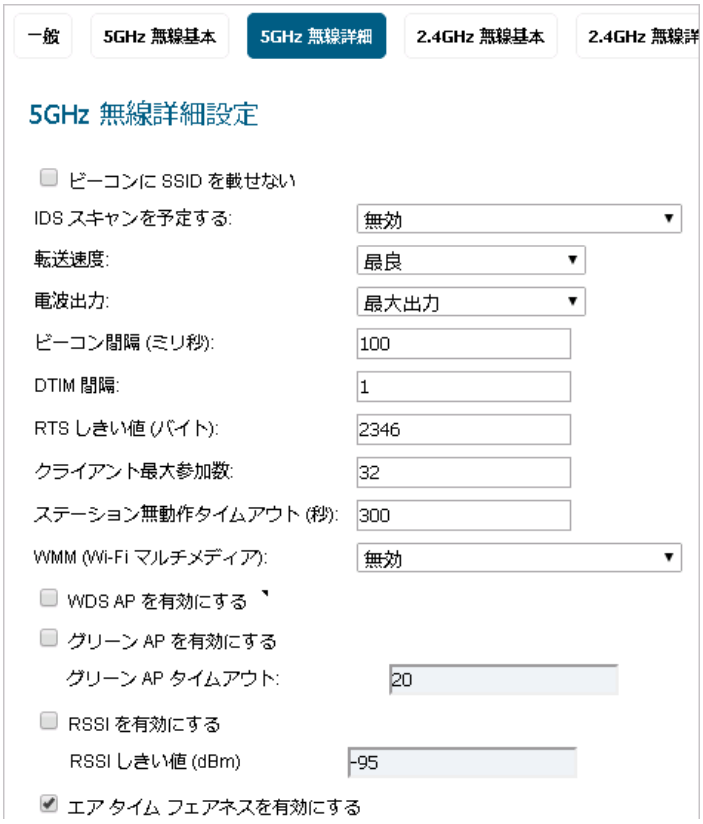
RSSI しきい値を構成するには:

1 「**管理 |接続 > アクセス ポイント> 基本設定**」に移動します。

2 「**SonicPoint/SonicWave プロビジョニング プロファイル**」までスクロールします。

3 SonicWave の「**設定**」アイコンを選択します。「**SonicPoint/SonicWave プロファイルの編集**」ダイアログが表示されます。

4 「**5GHz 無線詳細**」を選択します。



5 「**RSSI を有効にする**」を選択します。このオプションは既定では選択されていません。RSSI しきい値 (dBm) フィールドが利用可能になります。

6 「**RSSI しきい値 (dBm)**」フィールドにしきい値を入力します。この範囲は -35 から -95 で、既定値は **-95** です。

7 「**2.4GHz 無線詳細**」を選択します。

8 ステップ 5 から ステップ 6 を繰り返します。

9 「**OK**」を選択します。

RADIUS サーバ認証キャッシュ

この機能は、ローカルの SonicWave 装置に、選択した SonicWave 内でローカル RADIUS サービスを提供し、ネイティブ LDAP システムや Active Directory を含む社内ディレクトリ サービスと統合することで、ローカル RADIUS 認証サービスを提供するソリューションを提供します。

RADIUS サーバとしてローカル SonicWave を展開するには、NAT ポリシーとアクセス ルールを作成する必要があります。SonicWall ゲートウェイの NAT モジュールには、フェイルオーバーと負荷分散の方式があり、RADIUS サーバ プールが考慮されています。特定の条件が満たされている場合、ローカル RADIUS サーバとして使用される SonicWave をこのプールに追加できます。 つまり、複数のローカル RADIUS サーバがフェイルオーバー メカニズムを提供し、ネットワーク パフォーマンスを最適化します。

セキュリティ装置の電源投入時に、WLAN ゾーンでローカル RADIUS サーバが有効になっている場合は、RADIUS プール、NAT ポリシー、およびアクセス ルールが作成されます。RADIUS プール名は、RADIUS プール インタフェース名 + Radius Pool (例: X2 Radius Pool) です。それぞれの新しいアドレス オブジェクトは、SonicWave が RADIUS サーバとして機能するために自動的に作成され、サーバには SonicWave のインターフェース名と MAC アドレスで名前が付けられます (例: X2 18:b1:69:7b:75:2e)。

WLAN ゾーンを編集する場合は、NAT ポリシーとアクセス ルールを削除して再作成する必要があります。 ローカル RADIUS サーバを無効にしない限り、RADIUS プールは常に存在します。

インターフェースを変更する場合は、インターフェースが WLAN ゾーンにバインドされている場合は、NAT ポリシー、アクセスルール、および RADIUS プールを削除して再作成する必要があります。

Dell™ N シリーズ スイッチ サポート

トピック:

Dell™ N シリーズ スイッチについて

SonicOS 6.5.2.1 から、NSA 2600 および SOHO W プラットフォームを除くすべてのプラットフォームは、これらの Dell™ N シリーズ スイッチと N シリーズ統合をサポートします:

N1100	• N1108T-ON • N1108P-ON	• N1124T-ON • N1124P-ON	• N1148T-ON • N1148P-ON
N1500	• N1524 • N1524P	• N1548 • N1548P	
N2000	• N2024 • N2024P	• N2048 • N2048P	• N2128PX-ON
N3000	• N3024 • N3024P • N3024F	• N3048 • N3048P	• N3132PX-ON

セキュリティ装置やスイッチなどの重要なネットワーク要素を個別に管理する必要があることは、大きな苦労の 1 つです。Dell N シリーズ スイッチと Dell N シリーズ統合により、セキュリティ装置の管理インターフェースと GMS を使用して、セキュリティ装置と N シリーズ スイッチの統一的な管理が可能になります。Dell N シリーズ統合を用いて、N シリーズ スイッチのポートをセキュリティ装置の拡張インターフェースとみなすことができ、使用可能なインターフェースの数を増やすことができます。

N シリーズ スイッチと N シリーズ統合の基本的な違いの 1 つは、スイッチがセキュリティ装置によってプログラムされる方法です。

- N シリーズ統合では、セキュリティ装置がスイッチとの間で設定の差込み/取得するメカニズムとして XML API を使用します。
- N シリーズ統合は、スイッチを設定し、スイッチから設定を取得するメカニズムとして CLI を使用します。

N シリーズ統合対応 SonicWall セキュリティ装置プラットフォームの機能は、これらのプラットフォームでサポートされている N シリーズ統合の機能セットと同等であり、Dell X シリーズ スイッチ ソリューションに類似しています。SonicOS 6.5.2 では、最大 4 つの N シリーズ スイッチがサポートされています。 両方の N シリーズ スイッチが同じファイアウォールに統合されているシナリオでは、最大 4 つの N シリーズ スイッチを組み合わせることができます。N シリーズ スイッチのデイジーチェーン接続もサポートされています。

以下は、Dell スイッチ統合ソリューションの初期段階でサポートされている主要な機能です:

- 拡張スイッチとしての N シリーズ スイッチのプロビジョニング
- PortShield 機能
- N シリーズ スイッチのインターフェース設定の構成
- 基本的な N シリーズ スイッチのグローバル パラメータの管理
- GMSを使用した拡張スイッチの管理
- 高可用性とPortShield
- N シリーズ スイッチの診断サポート
- N シリーズ スイッチのデイジーチェーン

N シリーズ スイッチの設定

工場から出荷された N シリーズ スイッチは、既定で IP アドレスが設定されておらず、DHCP が有効になっています。以下の例は既定の設定で起動された N1524 スイッチの構成です:

```
console#show running-config

!Current Configuration:
!System Description "Dell Networking N1524, 6.2.5.3, Linux 3.6.5"
!System Software Version 6.2.5.3
!
configure
stack
member 1 1    ! N1524
exit
interface vlan 1
ip address dhcp
exit
snmp-server engineid local 800002a203f48e3807701e
exit

console#
```

N シリーズ スイッチが再起動したら、Dell Easy Setup Wizard を使用して初期設定を構成できます。ウィザードは、スイッチの初期設定をガイドし、できるだけ早く起動します。

メモ: 「Ctrl + Z」を入力することで、どの位置からでもセットアップ ウィザードを終了できます。

ヒント : セットアップ ウィザードをスキップして、CLI モードに入って手動でスイッチを設定することも可能です。

重要 : セットアップ ウィザードを実行するには、この質問に 60 秒以内に応答する必要があります :

```
Would you like to run the setup wizard (you must answer this question within
60 seconds)? (y/n) y
```

それ以外の場合、システムはデフォルトのシステム構成を使用して通常の稼働を続けます。空の起動構成でスイッチをリセットすると、Dell Easy Setup Wizard に戻ります。

Dell Easy Setup Wizardを使用して N シリーズ スイッチを設定する方法については、ご使用のスイッチの「*Dell Getting Started Guide*」を参照してください。

拡張スイッチとしての N シリーズ スイッチの配備

N シリーズ スイッチを外部の拡張スイッチとして SonicWall セキュリティ装置に追加するには、N シリーズ スイッチ上で SSH を有効にして、次のコマンドを入力する必要があります:

```
console(config)#crypto key generate dsa
console(config)#crypto key generate rsa
console(config)#ip ssh server
console(config)#crypto certificate 1 generate
console(config-crypto-cert)#key-generate
console(config-crypto-cert)#exit
```

メモ: 外部スイッチを追加する場合は、予約 VLAN ID の制限に注意してください。 仮想インターフェースが予約済み範囲内の VLAN ID を使用している場合は、外部スイッチを追加できません。

N シリーズ スイッチの完全な構成情報については、以下を参照してください:

http://www.dell.com/support/article/us/en/19/how10399/how-to-set-up-management-access-for-the-n2000-n3000-and-n4000-series-switches?lang=en

メモ: PoE 関連のフィールドは、PoE モデルの N シリーズ スイッチでのみ設定可能です。

アップリンク インターフェースの重要性

アップリンク インターフェースは、タグ付き/タグなしトラフィックを伝送するためのトランクポート設定として見ることができます。 ファイアウォール アップリンクとスイッチ アップリンク パラメータを持つ拡張スイッチが追加されると、ファイアウォール アップリンクとして設定されたセキュリティ装置上のポートと、スイッチ アップリンクとして設定された拡張スイッチ上のポートは、すべての IDV VLAN のタグ付きトラフィックを自動的に受信/送信するように設定されます 。 タグ付きトラフィックの IDV VLAN により、SonicOS はトラフィックの入力インターフェース、つまり PortShield ホスト インターフェースを取得できます。

インターフェースをファイアウォール アップリンクとして設定する場合、インターフェースは次のようになります:

- 物理インターフェースでなければなりません。仮想インターフェースは許可されません。
- スイッチ インターフェースである必要があります (セキュリティ装置の一部のインターフェースがスイッチに接続されていないプラットフォームでは、このようなインターフェースは除外されます）。

- PortShield ホストにできません (他のセキュリティ装置のインターフェースをポートシールドすることはできません）、また、PortShield メンバにすることはできません (別のセキュリティ装置インターフェースにポートシールドすることはできません）。
- ブリッジのプライマリまたはブリッジのセカンダリインターフェースにすることはできません。
- 子を持つことはできません (他の子インターフェースの親インターフェースにすることはできません）。

N シリーズ スイッチのプロビジョニング

N シリーズ スイッチをプロビジョンするには:

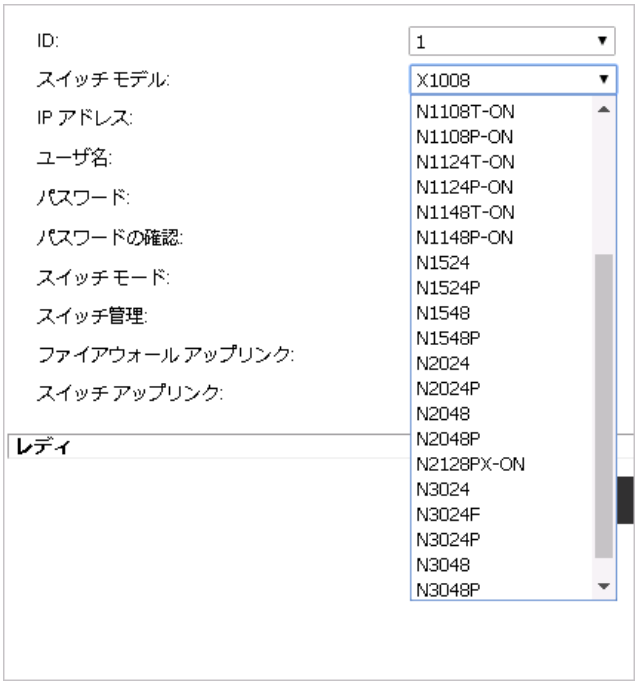
1 「**管理 |システム セットアップ> ネットワーク > PortShield グループ**」に移動します。

2 「**外部スイッチ設定**」を選択します。

3 「**スイッチの追加**」を選択します。「**外部スイッチの追加**」ダイアログが表示されます。

4 このスイッチの ID を「**ID**」から選択します。既定では「**1**」です。

5 スイッチのモデルを「**スイッチ モデル**」から選択します。



6 一般オプションの設定を終了します。

7 「**詳細**」を選択します。

8 詳細オプションの設定を終了します。

メモ: PoE オプションは PoE N シリーズ スイッチに対してのみ表示されます。

9 「**追加**」を選択します。「**外部スイッチ設定**」テーブルにスイッチが追加されます。

PortShield での拡張スイッチの設定

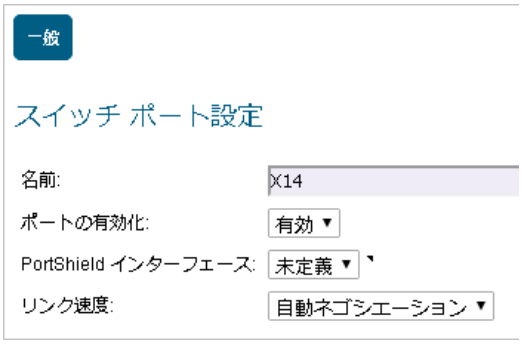
拡張スイッチを設定するには:

1 「**管理 |システム セットアップ> ネットワーク > PortShield グループ**」に移動します。

2 「**ポート画像**」を選択します。

3 設定するポートを選択します。

4 「**設定**」を選択します。「**スイッチポートを編集する**」ダイアログが表示されます。



5 オプションを設定します。

6 「**OK**」を選択します。

アプリケーション ベースのルーティング

アプリケーション ベースのルーティングは、トラフィックがルートテーブル内で指定された次のホップから代替パスを取得することを可能にする一種の PBF (ポリシーベース転送) ルールであり、通常はセキュリティまたはパフォーマンス上の理由から出力インターフェースを指定するために使用されます。

アプリケーション ベースのルート エントリが作成されると、最初はセキュリティ装置がアプリケーションを識別する十分な情報を持っていないため、ルート エントリを実行できません。より多くのパケットが到着すると、セキュリティ装置はアプリケーションを特定し、セッションのために保持されている内部エントリをアプリケーション シグネチャ キャッシュに作成します。同じ宛先 IP アドレス、宛先ポート、およびプロトコル ID を使用して新しいセッションを作成すると、セキュリティ装置は最初のセッションからアプリケーションを最初のセッションから同じと識別し、アプリケーション ベースのルートを適用できます。したがって、完全一致ではなく、同じアプリケーションではないセッションは、アプリケーション ベースのルートに基づいて転送することはできません。

この機能は、ゲートウェイ AV/アンチ スパイウェア/侵入防御/アプリケーション制御/ アプリケーション可視化がライセンスされ、「**管理 |ポリシー > ルール > アプリケーション制御**」でアプリケーション制御が有効になっている場合のみ利用可能です。

アプリケーション ベースのルート エントリを設定するには:

1 「**管理 |ポリシー > オブジェクト > 一致オブジェクト**」に移動します。

2 「**追加**」から「**一致オブジェクト**」を選択します。「**一致オブジェクトの追加**」ダイアログが表示されます。

3 「**一致オブジェクト種別**」から、以下を選択します。

- **アプリケーション種別リスト**
- **アプリケーションリスト**

4 一致オブジェクトの設定を完了します。

5 「**OK**」を選択します。

6 「**管理 |システム セットアップ> ネットワーク > ルーティング**」に移動します。

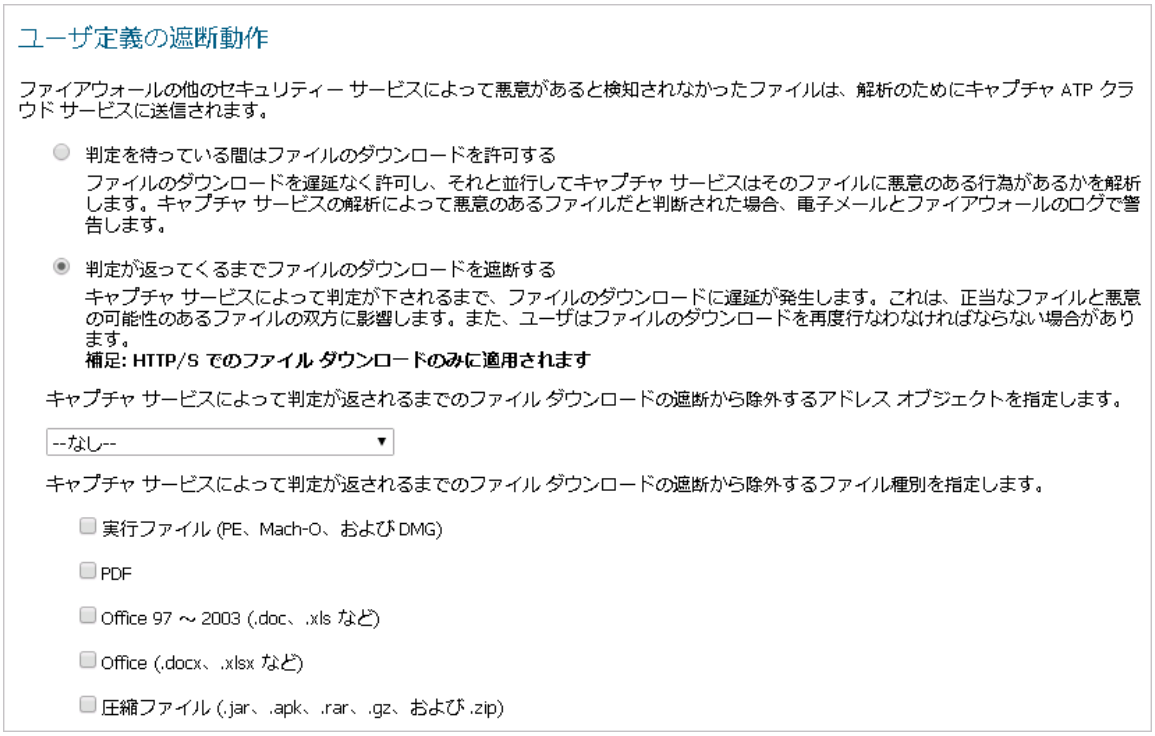
7 ルート ポリシーを作成します。

8 「**OK**」を選択します。

判定動作までのキャプチャ ATP 遮断強化

SonicOS では、キャプチャ ATP が特定のトラフィックまたはファイル種別をファイル ダウンロードの遮断から除外し、判定されるまでの間、ユーザ定義の遮断動作が可能になりました。これは、HTTP/S のファイル ダウンロードにのみ適用されます。

「**管理 | セキュリティ設定 > セキュリティ サービス > キャプチャ ATP**」ページの「**ユーザ定義の遮断動作**」セクションに、遮断動作をカスタマイズするためのオプションが含まれるようになりました。



DNS シンクホール

シンクホール サーバ、インターネット シンクホール、または BlackholeDNS とも呼ばれる DNS シンクホールは、それが表すドメイン名の使用を防止するために虚偽の情報を提供する DNS サーバーです。DNS シンクホールは、悪意のあるトラフィックを検出して遮断することに効果があり、ボットやその他の不要なトラフィックに対抗するために使用されます。

SonicOS にブラック/ホワイト リストを有効にして設定するための新しいページ「**管理 |システム セットアップ> ネットワーク > DNS セキュリティ**」が追加されました:

LAN バイパス

NSa 6650、SM 9250、SM 9450、および SM 9650 プラットフォームでは、ワイヤモードと L2 ブリッジングの両方でハードウェア (LAN) バイパスモードが有効になります。LAN バイパス モードが有効な場合の主な機能は:

- 再起動中に LBP 対応インターフェース間でトラフィックを通過させます。
- ファイアウォールの電源がオフになっている場合でも、それらの LBP 対応インターフェース間でトラフィックを通過させます。

NS*a* 9250、NS*a* 9450、および NS*a* 9650 プラットフォームの場合、インターフェース X26 と X27 の間で LAN バイパス機能を使用できます。NS*a* 6650 の場合、この機能は X0 と X1 の間で利用できます。

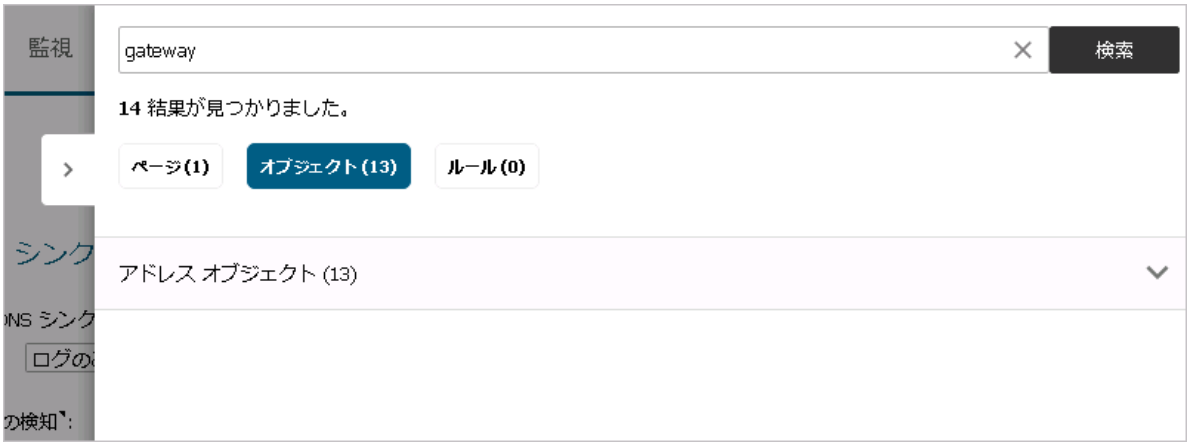
セカンダリ ストレージ デバイスでのファームウェア バックアップ

セカンダリ ストレージ デバイスを備えたすべての NS*a* シリーズ セキュリティ装置では、システム制限が許せば、SonicOS がファームウェアと構成設定ファイルのバックアップ (ファームウェア スナップショット) を行う機能をサポートするようになりました。

グローバル検索の強化

重要 : グローバル検索機能は、旧型の管理インターフェースではサポートされず、新型の表示でのみサポートされています。

グローバル検索機能は、オブジェクトやルールなどの構成オブジェクトと管理インターフェースページの動的検索を実行するようになりました。ページ検索結果には、メニュー項目の一部であるメイン ページへのリンクが含まれています。オブジェクトおよびルールの検索結果には、対応するオブジェクト/ルールの名前が表示され、一致する詳細が説明の一部としてリストされます。



メモ: 日本語版ファームウェアでは、ページ検索で日本語のキーワードがサポートされていますが、オブジェクトとルールの検索では英語のキーワードのみがサポートされています。

MGMT インターフェースでの高可用性ハートビート

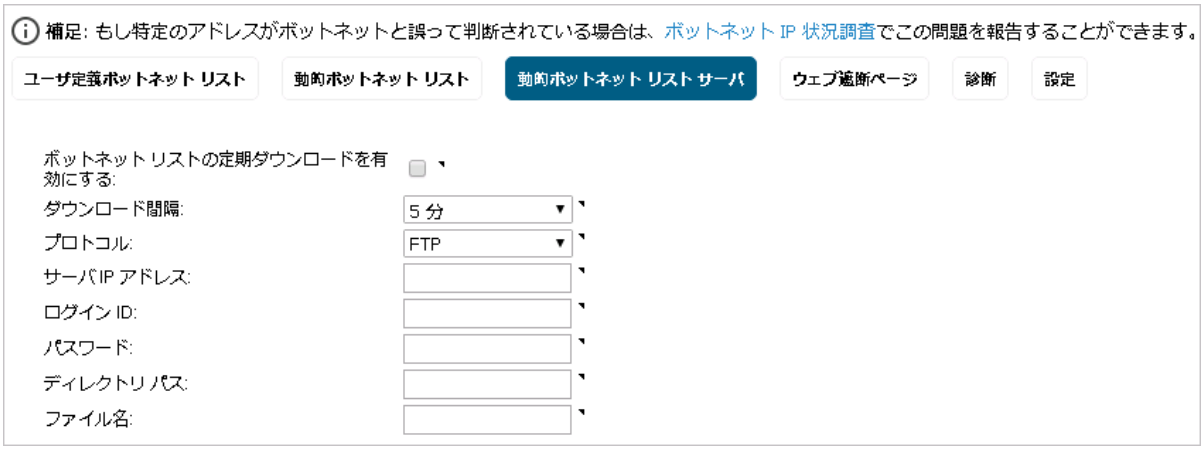
SonicOS セキュリティ装置では、HA 制御インターフェースに加えて、MGMT インターフェースを介して HA ペア間でハートビートを交換できるようになりました。

動的ボットネット HTTP 認証

SonicOS 6.5.0 の実装では、セキュリティ装置はパスワードで保護された URL を許可できませんでした。主な理由は、セキュリティ装置が HTTP GET を実行するときにトランザクションの状態を維持しないためです。このため、トランザクションはシングル ショットで行う必要があります。ただし、パスワードで保護されたサイトでは、サーバは HTTP 404 を返し、ユーザにはユーザ名とパスワードのダイアログが表示されます (通常のブラウザから使用する場合）。

SonicOS 6.5.2 では、動的ボットネット構成内で HTTP URL に対するユーザ名とパスワードが許可され、情報が HTTP ヘッダに送信されるので、GET 要求に必要な情報を持ちます。

この機能を有効にするために、「**管理 | セキュリティ 設定 > セキュリティ サービス > ボットネット フィルタ**」ページの「**動的ボットネット リスト サーバ**」セクションに「**ログイン ID**」と「**パスワード**」オプションが追加されました。



LHM RESTful API

SonicOS 6.5.2 は LHM RESTful API をサポートします。

LHM (Lightweight Hotspot Messaging) は、SonicWall 無線アクセス デバイス (SOHO W、TZ W シリーズ、または SonicWall セキュリティ装置に管理される SonicPoint など) と認証バックエンド (ABE) デバイス間の通信の方法と構文を定義します。ホットスポット ユーザを認証し、パラメータ的にバインドされたネットワーク アクセスを提供します。

RESTful API は、データの GET、PUT、POST、および DELETE のために HTTP 要求を使用するアプリケーション プログラム インターフェース (API) です。RESTful なウェブ サービスとも呼ばれる RESTful API は、ウェブ サービス開発で頻繁に使用されるアーキテクチャ スタイルであり通信アプローチである REST (Representational State Transfer) テクノロジに基づいています。

URI リスト グループ

SonicOS 6.5.2 では、許可リストと禁止リストの管理や Websense 除外のための URI リスト グループをサポートします。1 つのグループに複数の URI リスト オブジェクトを割り当て、そのグループを他のモジュール内で直接参照することができます。URI リスト グループはネストされた包含をサポートし、あるグループに他のグループを含めることができます。URI リストグループは、URI リストオブジェクトを使用できる場所であればどこでも使用できます。管理インターフェース、CLI、または GMS から URI リスト グループを設定できます。

「**管理 | ポリシー > オブジェクト > コンテンツ フィルタ オブジェクト**」に新しいセクションが追加されました。

最大で 128 の URI グループを設定できます。グループ名の最大長は 49 文字です。URI グループに最大 128 個のオブジェクト / グループを割り当てることができます。重複排除された URI の最大数は 5000 で、重複排除されたキーワードの最大数は 100 です。

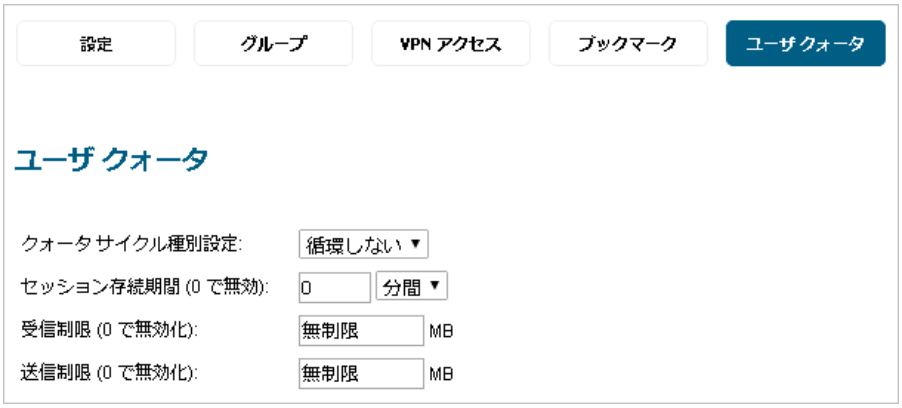
帯域幅クォータ制御

ユーザに対するクォータ制御機能は、ユーザのアカウントに基づいたクォータ制御を提供します。このクォータは、セッションの有効期間、または送信/受信トラフィック制限として指定できます。周期クォータでは、アカウント クォータに達したユーザは次のサイクル (日、週、または月) が始まるまでインターネットにアクセスできません。クォータ サイクルが非周期的のある場合、クォータに達したユーザはインターネットにアクセスできません。

以前は、ゲスト ユーザに対してのみクォータ制御をサポートしていました。SonicOS 6.5.2 では、すべてのローカル ユーザに対してもクォータ制御を指定できます。

ローカル ユーザに対してクォータを指定するには:

1 「**管理 |システム セットアップ> ユーザ > ローカル ユーザとグループ**」に移動します。
2 「**ローカル ユーザ**」を選択します。
3 「**追加**」を選択します。「**ユーザの追加**」ダイアログが表示されます。
4 「**ユーザ クォータ**」を選択します。



5 オプションを設定します。

6 「**OK**」を選択します。

フレキシブル記憶装置モジュール サポート

すべての NS*a* シリーズ プラットフォームは、内蔵記憶装置モジュールをサポートしています。このモジュールは、内蔵記憶装置モジュールのような記憶装置で、データの読み書きに使用されます。フレキシブル記憶装置モジュールは、各セキュリティ装置上で正常に有効化されている場合、複数のセキュリティ装置から使用できる共有装置です。フレキシブル記憶装置モジュールでは、セキュリティ装置のシリアル番号をディレクトリ名として最上位のディレクトリが作成されます。すべてのアプリケーションは、この最上位ディレクトリ内にサブ ディレクトリを作成し、そこにデータを格納します。

内蔵とフレキシブルの 2 つの記憶装置モジュールを利用できるようになり、機能に対して使用を選択できるようになりました。実行時のストレージの切り替えは、機能によっては利用できないため、再起動が必要な場合があります。たとえば、ログ監視機能の場合、記憶装置を別の記憶装置に切り替えるには再起動が必要です。ロギングの場合、記憶装置を選択するオプションは「**管理 | ログと報告 > ログ設定 > 基本設定**」ページで利用できます。両方のモジュールが使用可能な場合、既定では内蔵記憶装置モジュールが使用されます。

記憶装置が正常にマウントされている場合は、シリアル番号と統計情報が「**監視 | 現在の状況 > システム状況**」ページに表示され、そうでない場合は「**記憶装置利用不能**」が表示されます。

TACACS+ サポート

SonicOS 6.5.2 は、ユーザ認証用の TACACS+ (最新世代の Terminal Access Controller Access-Control System) をサポートするようになりました。TACACS+ の主な特徴は:

- 個別の認証、認可、および課金 (AAA) サービスを提供します。
- TCP を転送に使用します。
- 暗号化によって、TACACS+ ボディ全体が保護可能です。

TACACS+ を設定するには:

1 「**管理 |システム セットアップ> ユーザ > 設定**」に移動します。

2 「**ユーザ認証方式**」から、どちらかを選択します:

- **TACACS+**
- **TACACS+ + ローカル ユーザ**

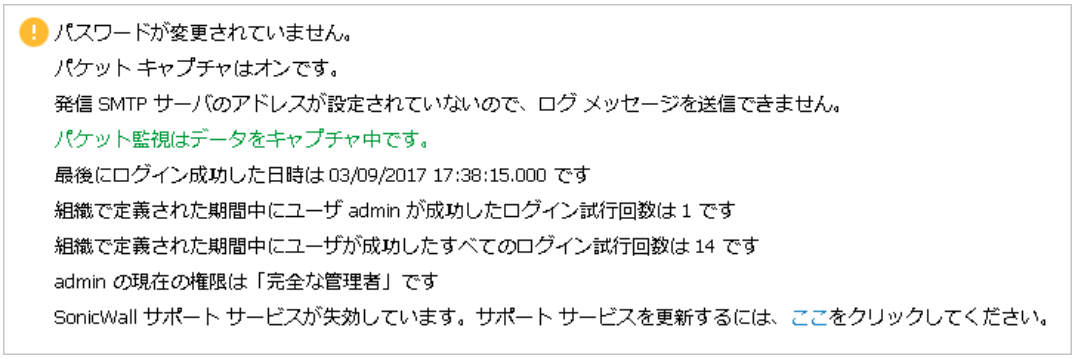
3 「**TACACS+ の設定**」を選択します。「**TACACS+ の設定**」ダイアログが表示されます。

4 オプションを設定します。

5 「**OK**」を選択します。

強化されたユーザ ログイン報告

SonicOS 6.5.2 は、「**監視 | 現在の状況 > システム状況**」ページへのログイン情報の報告をサポートするようになりました:



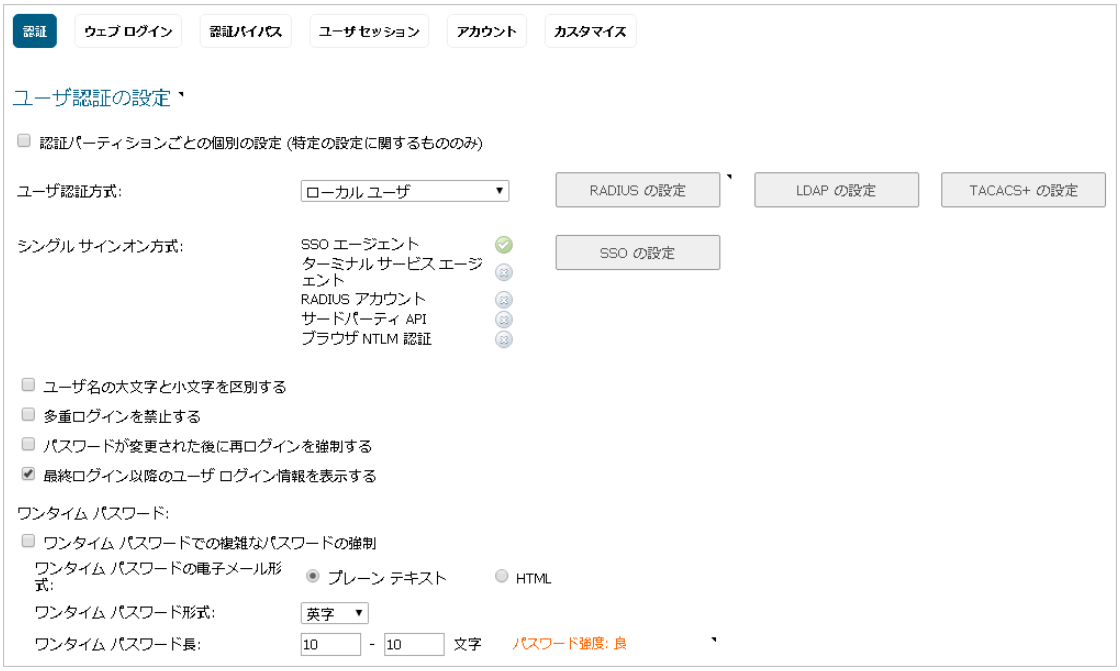
- 管理ユーザの最後のログオン タイム スタンプと場所
- 定義された期間中の管理ユーザの成功したログオン試行の合計数
- 定義された期間中のすべてのユーザの成功したログオン試行の合計数
- 現在の管理ユーザの特権

- 定義された期間中の管理ユーザの失敗したログオン試行の合計数
- 前回のログオン以降の管理ユーザの権限変更の通知

ログイン情報の報告を有効にするには:

1 「**管理 |システム セットアップ> ユーザ > 設定**」に移動します。

2 「**認証**」を選択します。



3 「**最終ログイン以降のユーザ ログイン情報を表示する**」を選択します。

4 「**適用**」を選択します。

WeChat ソーシャル認証

SonicOS 6.5.2 は中国で非常に有名なソーシャル アプリである WeChat をサポートするようになりました。

アクセス ポイント可視化の強化

SonicOS 6.5.2 では、アクセス ポイント (AP： SonicPoint および SonicWave 装置) の状況が、表形式とグラフやチャートなどのグラフ形式の両方で表示されるようになりました。問題診断と状況監視を支援するために、AP のリアルタイム状況と履歴をグラフとして表示することができます。

- CPU とメモリの使用率
- 1 つまたは複数の AP のクライアント速度
- 各クライアントの速度、OS 種別、およびホスト名
- 1 つの AP の異なるステーションの状況と異なる AP の状況

LAG に対する VLAN 拡張

リンク統合 (LAG) により、複数のリンクをより大きな 1 つの仮想パイプに結合してより太い結合帯域幅を持つことができるように、2 つ以上のリンクを持つデバイスを相互接続することができます。2 つのデバイス間に複数のリンクが存在するため、1 つのリンクに障害が発生しても、トラフィックは中断することなく他のリンクを介してシームレスに転送されます。複数のリンクを用いて、トラフィックも均一に分散されるような方法で負荷分散されます。

この拡張により:

- VLAN を追加 / 削除する前に、LAG を分離または削除する必要はありません。この構成により、LAG やその他の LAG に設定されている VLAN に関連する現在のトラフィックを中断せずに、既存の LAG に VLAN を追加したり、既存の LAG から VLAN を削除することができます。
- LAG の任意のメンバーに VLAN を追加 / 削除することが可能で、それは LAG の他のメンバーに明示的に追加 / 削除する必要なしに、LAG の他のすべてのメンバーに自動的に適用されます。

SonicOS 6.5.2 では、NS*a* シリーズ、NSA シリーズ、および SuperMassive シリーズの各プラットフォームで LAG 上の拡張 VLAN 機能サポートが利用可能です。

修正された問題点

このセクションでは、本リリースで修正された問題点のリストを示します。

アクセス ポイント

修正された問題点	問題番号
SonicWave アクセス ポイントが、SonicOS で無効にされているにもかかわらず、有効になっていて操作可能です。	197080
SonicWave 231c/224w/231o のファームウェアがアップロードできません。	201785
「接続性 > アクセス ポイント」のタブのさまざまなページの最後にフィールドがありません。	201730
WPA2-自動-PSK と PMF 必須 が 5GHz と 2.4GHz どちらかの無線に設定されている場合、5GHz と 2.4GHz どちらの無線も検出できません。	201412
Huawei E3372s-153 がダイヤルアップできません。	201170

API

修正された問題点	問題番号
SonicWall 管理者で API を使用して設定できません。 SonicWall 管理者で API を使用して設定モードに入るときに発生します。設定モードに変更されず、設定しようとすると Unauthorized と表示されます。	201747
先制機能を使用できません。 既存の管理者ユーザを先制しようとしたときに発生します。先制を試みたユーザは非設定モードのままで、設定しようとすると ”An administrator is already logged in for configuration” というメッセージが表示されます。	200271

AppFlow

修正された問題点	問題番号
AppFlow ログ: AppFlow Server2 または GMSFlow Server2 としてデータ ソースを選択すると、ローカル データ ソースにリダイレクトされます。	201808
AppFlow Monitor: URL (URL、ドメイン名、評価) のデータがありません。	198988

LDAP

修正された問題点	問題番号
LDAP からインポートする際に場所別にユーザをフィルタするために使用するフィールドがありません。	195781

ログ

修正された問題点	問題番号
NS*a* 3650/4650 の「**管理	ログと報告 > ログ設定**」ページで設定の保存に失敗します。	201315

ネットワーク

修正された問題点	問題番号
TI インターフェースにバインドされたスタティック ルートを追加するためのアクセス ルールの自動追加が機能しません。	201707
新しい追加された個別 NAT ポリシーの優先度が、既定のものよりも低くなっています。	201255
DNS サーバの応答が破棄されます。	200277
NetBIOS ポリシーを追加した後で、名前クエリ応答が破棄されます。	200221
有効化された RIP が、セキュリティ装置の再起動後に無効を示します。	200129
NAT ポリシーに対する MAC 上書きが、上書きした MAC を持つ個別 NAT ポリシーの追加に失敗し、"エラー: NAT ポリシーを変更できません。" エラーが発生します。	199984
既定の NAT ポリシーを編集 / 削除 / 無効にすると、”エラー: NAT ポリシーを変更できません。” エラーが発生します。	199855

SSL VPN

修正された問題点	問題番号
WLAN というゾーンをクリックして WLAN ゾーンで SSLVPN を有効にしようとすると、複数のエラーが表示されます。	201095
IPv6 SSL VPN が LACP グループのインターフェース IP に接続に失敗し、コンソール メッセージ ”dp_stack_output:1259: Need to free this WQE!!! “ が表示されます。	194566

システム

修正された問題点	問題番号
10G ポートが無効になっていると、セキュリティ装置が再起動されることがあります。	206309
M2 ストレージのシリアル番号がバックエンドに追加されていない場合に、セキュリティ装置が再起動されます。	201359

SonicOS API

修正された問題点	問題番号
DNS が手動で構成されていると、DNS を WAN から引き継ぐように構成を戻すことができません。	199430

ユーザ インターフェース

修正された問題点	問題番号
ウィザードで、ポート構成ページの X8-X15、X26-X27 銅ポートに対して 2.5G 速度がありません。	200798
グローバル検索: IE11 で何か検索したときに、検索レコードが 0 を表示します。	201407

ユーザ

修正された問題点	問題番号
ローカル ユーザのパスワードが正しく変更できません。	200972
SM9650 でユーザが作成できずにエラー メッセージが表示されます。	200467

無線

修正された問題点	問題番号
WLAN ゾーンのゲスト サービス タブの DAT を有効にするオプションが表示されません。	201733
ゲスト ユーザのログイン一意性機能が動作しません。	201625
6.5.2.1-8n、6.5.1.1-36n でキャプティブ ポータル認証が 失敗すします。	201305

X シリーズ スイッチ

修正された問題点	問題番号
1 つのスイッチ上のファイアウォール アップリンクと別のスイッチ上の専用リンクとの間の VLAN の重複ができません。	200805

確認されている問題点

このセクションでは、本リリースで確認されている問題点のリストを示します。

AV クライアント

確認されている問題点	問題番号
AV クライアント除外リストの設定が消失します。	206384

DPI SSL

確認されている問題点	問題番号
クライアント DPI-SSL: コモン ネーム .sonicwall.com を拒否する設定で、* .sonicwall.com を含む ウェブ サイトにアクセスすると、それらのウェブ サイトが DPI 遮断から除外されることがあります。	201605
クライアント DPI SSL: コモン ネームに対するサーバの認証スキップが動作しません。	201525
CFS 種別に基づいた除外のスキップが動作しません。	199845

ネットワーク

確認されている問題点	問題番号
IPv6 BGP 近隣者発見が失敗します。 IPv4 BGP 近隣者発見が MD5 を使用して確立されている場合に発生します。	205025
NSA 6650 の 1 / 2.5G および 1 / 2.5 / 5 / 10G SFP ポートに対して、一部のリンク速度オプションが不足しています。	199992

PortSheild

確認されている問題点	問題番号
N シリーズ スイッチ: 専用のアップリンク トポロジで再起動すると、PortShield ポートの設定が失われます。 子スイッチと親スイッチで構成されている場合に発生します。	205491

ユーザ

確認されている問題点	問題番号
LDAP サーバからインポートされたローカルユーザが、再起動後に消失します。 ユーザの 1 人が編集された場合に発生します。	205790
「**管理 | システム セットアップ> ネットワーク > ウェブ プロキシ**」のリストにユーザ プロキシ サーバを追加できません。	205551
ゲストアカウントに対する「**初回ログインの時点でアカウント有効期限を有効にする**」オプションを有効または無効にすることができません。	205520
クォータ期間が LDAP ユーザに適用されません。	205185
LDAP サーバからローカル ユーザ データベースにユーザをインポートできません。	201713
ドメイン\ユーザとして入力されたホスト名が RADIUS アカウント サーバ リストから削除できません。	200056

無線

確認されている問題点	問題番号
WLAN クライアントが、LHM サーバによって正常に認証された後に、要求されたウェブサイトにリダイレクトされません。	203499

日本語版特有の問題点

確認されている問題点	問題番号
TZ Wireless/SOHO Wireless 装置に日本語以外のファームウェアをアップロードし、工場出荷時の設定で起動した場合、無線のチャンネル数が制限されます。	-
「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。 「プロキシサーバを通してシグネチャをダウンロードする」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、シグネチャのダウンロード機能は正しく動作します。	83453
現在使用されているファームウェアのバージョンが、本リリースのファームウェアに対して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る場合、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状態でのみそれをサポートします。	-
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。	

システムの互換性

このセクションでは、ハードウェアおよびソフトウェアの本リリースとの互換性に関する追加情報を提供します。

ワイヤレス 3G/4G ブロードバンド機器

SonicOS 6.5.2 では、さまざまな種類の PC カード、USB 機器、および無線サービスのプロバイダがサポートされます。サポートされる機器の最新のリストについては、以下のリンク先を参照してください。
https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240

GMS のサポート

SonicOS 6.5.2 が稼働している SonicWall セキュリティ装置の SonicWall グローバル管理システム (GMS) 管理には、SonicOS 6.5.2 の新機能を使用するファイアウォールの管理用に GMS 8.4 が必要です。SonicWall GMS 8.3 SP1は、SonicOS 6.2.9.2 以前のリリースが持つすべての機能の管理をサポートしています。

WAN 高速化/WXA のサポート

SonicWall WXA シリーズの装置 (WXA 6000 ソフトウェア、WXA 500 Live CD、WXA 5000 仮想装置、WXA 2000/4000 装置) では、SonicOS 6.5.2 が稼働する SonicWall セキュリティ装置と共に使用することがサポートされています。推奨される WXA ファームウェアのバージョンは、WXA 1.3.2 です。

ブラウザのサポート

可視化機能を備えた SonicOS は、最近のほとんどのブラウザがサポートする HTML5 などの先端のブラウザ技術を使用しています。SonicWall では、SonicOS の管理に最新の Chrome、Firefox、Internet Explorer、または Safari のいずれかのブラウザを使用することを推奨します。このリリースでは、以下のウェブブラウザがサポートされています。

- Chrome 45.0 以降
- Firefox 25.0 以上
- IE Edge または IE 10.0 以上
- 非 Windows マシンで動作する Safari 10.0 以上

メモ: Windows マシンでは、Safari による SonicOS の管理はサポートされていません。

メモ: SonicWall 装置のシステム管理には、モバイル デバイスのブラウザは推奨されません。

製品ライセンス

SonicWall セキュリティ サービスのすべての機能と利点、ファームウェア アップデート、および技術サポートを有効にするためには、SonicWall ネットワーク セキュリティ装置を MySonicWall 上で登録する必要があります。MySonicWall アカウントへのログインまたは登録は、https://mysonicwall.com/ から行います。

アップグレード情報

最新ファームウェアの取得方法、SonicWall 装置のファームウェア イメージのアップグレード方法、および他の装置から構成設定をインポートする方法については、サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation) から入手できる『*SonicOS 6.5.2 アップグレード ガイド*』を参照してください。

SonicWall のサポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様や、トライアル バージョンをお持ちのお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、https://www.sonicwall.com/ja-jp/support に移動します。

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- ビデオ チュートリアルを視聴する。
- MySonicWall にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートへの連絡方法は、https://www.sonicwall.com/ja-jp/support/contact-support をご覧ください。

凡例

警告: 物的損害、けが、または死亡に至る可能性があることを示しています。

注意: 手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

重要、メモ、ヒント、モバイル、またはビデオ: 補足情報があることを示しています。

最終更新日: 2018 年 8 月

232-004445-00 Rev A