SonicWall® SonicOS 6.5 接続

管理

SONICWALL®

目次

第 1 部 接続性 | VPN

第 2 部 接続性 | SSL VPN

第 3 部 接続性 | アクセス ポイント

第 4 部 接続性 | 無線

第 6 部 接続性 | 付録

第 1 部

接続性 | VPN

- VPN の概要
- サイト間 VPN
- VPN 自動プロビジョニング
- トンネル インターフェースルート ベース VPN
- VPN の詳細設定
- VPN を越えた DHCP の設定
- L2TP サーバと VPN クライアント アクセスの設定
- AWS VPN

1

VPN の概要

VPN オプションは、VPN ポリシーの表示と設定の機能を提供します。さまざまな種類の IPsec VPN ポリシーを設定できます。例えば、GroupVPN などのサイト間ポリシーやルート ベースのトンネル インターフェース ポリシーを設定できます。この種のポリシーに対する設定の詳細については、以下のセクションに移動してください。

- サイト間 VPN
- VPN 自動プロビジョニング
- トンネル インターフェースルート ベース VPN

このセクションでは、VPN の種類、選択可能なセキュリティ オプション、「**管理**」ビューの「**VPN > 基本設定**」ページのインターフェースについて説明します。後続の各セクションでは、サイト間 VPN とルート ベース VPN、詳細設定、VPN を越えた DHCP、および L2TP サーバの設定方法について説明します。

メモ：SonicOS 6.5.3 以降では、「**管理 | システム設定 | 装置 > 基本設定**」ページの「**無線制御モード**」が「**フル機能ゲートウェイ**」または「**無線なし**」に設定されているとき、**VPN** ページの機能を利用できます。「**無線制御モード**」で「**無線制御のみ**」が有効になっている場合、**VPN** ページで VPN ポリシーを追加して管理する機能は使用 ***できません***。詳細については、『*SonicOS 6.5 システム設定* 管理ガイド』を参照してください。

トピック:

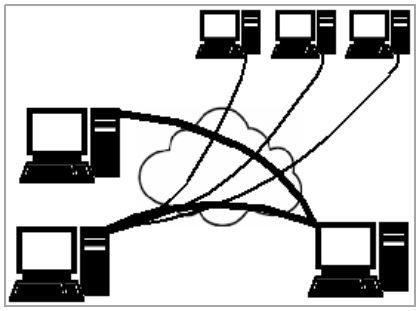
- 仮想プライベート ネットワークについて
- VPN の種類
- VPN のセキュリティ
- VPN ベースの設定と表示
- IPv6 VPN の設定
- VPN が自動的に追加するルール コントロール

仮想プライベート ネットワークについて

仮想プライベート ネットワーク (VPN) では、パブリック インターネットを介して 2 台以上のコンピュータ、または保護されたネットワーク間をセキュリティ保護された手段で接続できます。VPN では、正しい通信相手との情報の送受信を保証するために、認証が実施されます。情報を送受信途中の閲覧や改ざんから保護するためのセキュリティも確保されます。

VPN は、セキュリティ保護されたトンネルをインターネット経由で確立します。このトンネルは、専用線接続、仮想トンネリングプロトコル、または通信暗号化の利用を通じた、地点間の仮想接続です。これはいつでも柔軟に変更でき、ノードを追加したり、変更したり、まとめて除去したりできま

す。また、VPN のインターネット インフラストラクチャには既存のものを使えるため、コストをかなり低く抑えることもできます。



VPN は、リモート アクセス (ユーザのコンピュータを企業のネットワークに接続する機能) とサイト間アクセス (2 つのネットワークを接続する機能) のどちらもサポートできます。VPN はまた、2 つの同種のネットワークを、異種の中間ネットワークを通じて接続するためにも使用されます。例えば、2 つの IPv6 ネットワークを、IPv4 ネットワークを通じて接続するなどです。

VPN システムには、以下のような内容によって分類できます。

- トラフィックのトンネル化に使用されるプロトコル
- トンネルが終了する場所。例えば、カスタマー エッジやネットワーク プロバイダ エッジなど
- 接続トポロジの種別 (サイト間接続、ネットワーク間接続など)
- 提供されるセキュリティのレベル
- 接続ネットワークに関する OSI 参照モデルにおける位置づけ。例えば、第 2 層データリンク層か、第 3 層ネットワーク層か、など
- 同時接続数

VPN の種類

各種の VPN プロトコルが設定・使用可能です。

- IPsec VPN
- VPN を越えた DHCP
- IPsec を利用した L2TP
- SSL VPN

IPsec VPN

SonicOS は、IPsec VPN の作成および管理をサポートしています。これらの VPN は、主として **VPN > 基本設定**と **VPN > 詳細設定**表示の **管理** で設定可能です。

IPsec (インターネットプロトコルセキュリティ) は、標準に基づいてセキュリティを提供するプロトコルで、当初は IPv6 のために開発されたものですが、IPv4 および L2TP においても広く利用されています。その設計は、認証、統合性、秘密保持といったほとんどのセキュリティ目標に合致しています。IPsec は暗号化を利用し、IP パケットを IPsec パケットにカプセル化します。カプセル化からの取り出しはトンネル化の終端点で行われ、IP パケットが復号化されて意図された送り先に向けて送信されます。

IPsec のメリットは、個別ユーザのコンピュータを変更する必要なしにセキュリティ上の処置に対処できることです。IPsec は、2 種類のセキュリティサービスを提供します。

- データ送信者の認証を基本的に許可する認証ヘッダー (AH)
- データ送信者の認証およびデータの暗号化の両方をサポートするカプセル化セキュリティペイロード (ESP)

IPsec を使用することで、ポリシー ベースの VPN (サイト間) 、ルート ベースの VPN トンネル、または、レイヤ 2 トンネリング プロトコル (L2TP) を作成できます。

VPN を越えた DHCP

SonicOS VPN トンネルの反対側にある DHCP サーバから IP アドレスリースを取得するようにファイアウォールを設定可能にします。ネットワークの配備によっては、1 つの論理 IP サブネットにすべての VPN ネットワークを置き、1 つの IP サブネットアドレススペース上ですべての VPN ネットワークが見えるようにすることが望ましい場合があります。これにより、VPN トンネルを使用するネットワークの IP アドレス管理が容易になります。

リモート サイトおよび中央サイトのファイアウォールは、サイト間の最初の DHCP トラフィックおよびそれ以降の IP トラフィックに対して、VPN トンネル用に設定されます。リモートサイトのファイアウォールは、VPN トンネルを通して DHCP ブロードキャストパケットを渡します。中央サイトのファイアウォールは、リモートネットワーク上のクライアントからの DHCP パケットを、中央サイトの DHCP サーバにリレーします。

IPsec を利用した L2TP

レイヤ 2 トンネルプロトコル (L2TP) は、VPN をサポートするためか、ISP によるサービス提供の一部として使用される、トンネルプロトコルです。L2TP は、それ自体では暗号化も機密性も提供しません。L2TP は機密性がないため、しばしば IPsec と共に実装されます。L2TP/IPsec VPN を設定する一般的な手順は以下のとおりです。

1. 一般的には、インターネット鍵交換 (IKE) を通じて IPsec セキュリティアソシエーション (SA) をネゴシエートします。それは UDP ポート 500 を通じて実行され、共有パスワード (「事前共有鍵」ともいいます)、公開鍵、または両側における X.509 証明書を通常は使用します。ただし、その他の鍵交換方法も存在します。
2. 転送モードにおけるカプセル化セキュリティペイロード (ESP) 通信を確立します。ESP の IP プロトコル番号は 50 です (TCP の 6 や UDP の 17 と比較してください) この時点で、安全なチャンネルは確立されましたが、トンネリングは実現していません。
3. SA の両エンドポイント間で、L2TP トンネルをネゴシエートして確立します。実際のパラメータのネゴシエーションは SA の安全なチャンネルを通じて、IPsec の暗号化の下で実行されます。L2TP は UDP ポート 1701 を使用します。

手順が完了すると、両エンドポイント間の L2TP パケットは、IPsec でカプセリングされます。L2TP パケット自体は IPsec パケットにカプセリングされて隠されてしまうため、内部のプライベートネットワークに関する情報を暗号化されたパケットから収集することはできません。また、両エンドポイント間のファイアウォールにおいて、UDP ポート 1701 を解放する必要はありません。なぜなら、内部のパケットは IPsec データが復号化されて内部のパケットが取り出されるまで実行されず、それは両エンドポイントにおいてのみ実行されるからです。

SSL VPN

SSL VPN (Secure Socket Layer Virtual Private Network) は VPN の一形態で、標準的なウェブブラウザで使用できます。従来の IPsec VPN とは対照的に、SSL VPN はエンドユーザのコンピュータに専用のクライアントソフトウェアをインストールする必要がありません。ウェブアプリケーション、クライアント/サーバアプリケーション、および内部ネットワーク接続に、リモートユーザがアクセスするために使用できます。

SSL VPN は、ユーザがウェブブラウザを使用して接続する対象となる、1 つ以上の VPN 装置から構成されます。ウェブブラウザと SSL VPN 装置との間の通信は、SSL プロトコルか、その後継である Transport Layer Security (TLS) プロトコルで暗号化されます。SSL VPN は、さまざまなコンピュータを使用してさまざまな場所からリソースにアクセスする広い範囲のユーザに対して、汎用性、取扱の簡単さ、きめ細かい管理性を提供します。SSL VPN には大きく分けて 2 種類あります。

- SSL ポータル VPN
- SSL トンネル VPN

SSL ポータル VPN は、ユーザが安全に複数のネットワークサービスを利用できるように、ウェブサイトに対して単一の SSL 接続を可能にします。サイトは、他の多くのリソースにつながる扉 (単一のページ) であるため、ポータルと呼ばれます。リモートユーザは、最新のウェブブラウザを使用して SSL VPN ゲートウェイにアクセスし、ゲートウェイがサポートする認証方法を使ってゲートウェイにユーザ自身を識別させます。そして、他のサービスのポータルとして働くウェブページにアクセスすることができます。

SSL トンネル VPN は、SSL の下で働くトンネルを通じて、ウェブベースでないアプリケーションやプロトコルを含めた複数のネットワークサービスに、ウェブブラウザから安全にアクセスできるようにします。SSL トンネル VPN には、SSL ポータル VPN ではアクセスできない機能を提供できるような、アクティブコンテンツを取り扱うことができるウェブブラウザが必要です。アクティブコンテンツの例としては、Java、JavaScript、Active X、Flash アプリケーションまたはプラグインなどがあります。

SSL が使用するプログラム層は、インターネットのハイパーテキスト転送プロトコル (HTTP) 層と転送制御プロトコル (TCP) 層との間に位置しています。SSL には RSA の公開鍵/秘密鍵暗号化方式が使用され、この暗号化方式を使用する際にはデジタル証明書も使用されます。SRA/SMA 装置は、SSL を使用して VPN トンネルのセキュリティを保護します。SSL VPN のメリットの 1 つは、ほとんどのウェブ ブラウザに SSL を組み込めることです。その際に特別な VPN クライアント ソフトウェアやハードウェアは必要ありません。

メモ：SonicWall が製造する Secure Mobile Access (SMA) 装置は、SonicOS の稼働する SonicWall ネットワーク セキュリティと装置と連携させて使うことも、それとは別個に使うこともできます。SonicWall SMA 装置の詳細は、https://www.sonicwall.com/ja-jp/products を参照してください。

VPN のセキュリティ

IPsec VPN トラフィックは、次の 2 つのフェーズでセキュリティ保護されます。

1. **認証**: 第 1 フェーズでは、公開鍵と秘密鍵のペアのうちの公開鍵部分の交換によって、トラフィックの送信者および受信者の認証を確立します。このフェーズが正常終了しないうちは、VPN トンネルを確立できません。
2. **暗号化**: VPN トンネル内のトラフィックは、AES や 3DES などの暗号化アルゴリズムを使用して暗号化されます。

手動鍵を使用する場合 (VPN 内の各ノードに同じ値を入力する必要があるため)、VPN メンバー認証情報およびデータ暗号化/復号化情報を交換する際には、認証情報 (鍵) の交換および VPN トンネル確立のための IKE (インターネット鍵交換) プロトコルが使用されます。SonicOS では、以下の 2 つのバージョンの IKE がサポートされます。

IKE バージョン 1 (IKEv1)	2 つのフェーズから成る処理によって、VPN トンネルのセキュリティを保護します。最初に 2 つのノードが互いに認証し合い、次に暗号化の方法をネゴシエートします。 IKEv1 の詳細は、IKE を最初に定義した 3 つの仕様書に記載されています。RFC2407、RFC2408、RFC2409 です。次のウェブで閲覧できます。 • http://www.faqs.org/rfcs/rfc2407.html - *The Internet IP Security Domain of Interpretation for ISAKMP* • http://www.faqs.org/rfcs/rfc2408.html - *RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)* • http://www.faqs.org/rfcs/rfc2409.html - *RFC 2409 - The Internet Key Exchange (IKE)*
IKE バージョン 2 (IKEv2)	IKEv2 は新しい VPN ポリシーに対する既定の種別です。その理由は、改良されたセキュリティ、簡素化されたアーキテクチャ、強化されたリモートユーザ向けサポートです。VPN トンネルは、2 組のメッセージ交換を使用して初期化されます。1 組目のメッセージは、暗号化アルゴリズムをネゴシエートし、ナンス (反復したメッセージを防ぐために生成し送信されるランダム値) を交換して、公開鍵交換を実行します。2 組目のメッセージは、以前のメッセージを認証し、識別情報および証明書を交換して、最初の CHILD_SA (セキュリティ アソシエーション) を確立します。これらのメッセージの一部は、最初の交換で確立された鍵によって暗号化され整合性が保全されます。 その結果、識別情報が盗聴から隠蔽され、あらゆるメッセージの全フィールドが認証されます。 IKEv2 の詳細は、仕様書 RFC4306 に記載されています。次のウェブで閲覧できます。http://www.ietf.org/rfc/rfc4306.txt

重要：IKEv2 には IKEv1 との互換性はありません。IKEv2 を使用する場合、トンネルを確立するには、VPN 内のすべてのノードに IKEv2 を使用する必要があります。
IKEv2 では、VPN を越えた DHCP がサポートされません。

VPN セキュリティの詳細については、以下を参照してください。

- IKEv1 について
- IKEv2 について
- IKEv2 のモビリティおよびマルチホーム プロトコル (MOBIKE)
- IPsec (フェーズ 2) プロポーザルについて
- Suite B 暗号化について

IKEv1 について

IKEv1 では、認証情報を交換するために 2 つのモードが使用されます。

- **メイン モード**: VPN を起動するノードまたはゲートウェイは、受信側のノードまたはゲートウェイに問い合わせて、認証方式、公開鍵、および識別情報を交換します。この処理では通常 6 つ

のメッセージを送受信する必要があります。メイン モードでは、認証メッセージが次のような順序で処理されます。

1) 始動者が自らサポートしている暗号化アルゴリズムのリストを送信する
2) サポートされている暗号化アルゴリズムのリストを、応答側が使用して応答する
3) 相互にサポートされている最初の暗号化アルゴリズム用の公開鍵 (Diffie-Helman 公開/秘密鍵のペアの一部) を始動者が送信する
4) 応答側が同じ暗号化アルゴリズムの公開鍵を使用して応答する
5) 始動者が識別情報 (通常は証明書) を送信する
6) 応答側が識別情報を使用して応答する

- **アグレッシブ モード**: 認証時に交換されるメッセージの数を半減するために、どの暗号化アルゴリズムを使用したらよいかについてのネゴシエーションが省略されます。ある特定のアルゴリズムを始動者が提案すると、応答側はそのアルゴリズムをサポートしているかどうかについての応答を返します。 例えば、次のようになります。

  1) 始動者が自らの公開鍵を使用/送信するための暗号化アルゴリズムを提案する
  2) 応答側が公開鍵および識別証明を使用して応答する
  3) 始動者が識別証明を送信する 認証後は、VPN トンネルが 2 つの SA を使用して確立されます。それぞれ、一方のノードから他方のノードへの SA です

IKEv2 について

IKE バージョン 2 (IKEv2)　は、セキュリティ アソシエーション (SA) のネゴシエーションおよび確立のためのより新しいプロトコルです。セカンダリ ゲートウェイは IKEv2 をサポートします。IKEv2 は新しい VPN ポリシーに対する既定のプロポーザル種別です。

メモ：IKEv2 には IKEv1 との互換性はありません。IKEv2 を使用する場合、トンネルを確立するには、VPN 内のすべてのノードに IKEv2 を使用する必要があります。IKEv2 では、VPN を越えた DHCP がサポートされません。

IKEv2 は IKEv1 より以下の利点があります。

- より高い安全性
- より高い信頼性
- より簡易化
- より高速
- 拡張性
- 接続を確立するための、より少ないメッセージ交換
- EAP 認証サポート
- MOBIKE サポート
- ビルトイン NAT トラバーサル
- 既定でキープアライブが有効

IKEv2 では、上記以外に IP アドレスの割り当ておよび拡張認証プロトコル (EAP) もサポートすることにより、いくつかの認証方式やリモート アクセスのシナリオを可能にします。IKEv2 を使用することにより、セキュリティ アソシエーションの確立に要するメッセージ交換の回数が IKEv1 のメイン モードに比べて大幅に減少すると同時に、IKEv1 のアグレッシブ モードに比べてセキュリティが強化され柔軟性が高まります。これにより、鍵を再設定する際の遅延が低減します。VPN の拡大に伴って複数のノードまたはゲートウェイ間に含まれるトンネルが増えると、IKEv2 は各トンネルに要するセキュリティ アソシエーションの数を減らすことによって、帯域幅の必要量を低く抑え、システム管理の諸経費を軽減します。

IKEv2 内のセキュリティ アソシエーション (SA) は子 SA と呼ばれており、VPN トンネルの有効期間中はいつでも個別に作成、変更、削除することができます。

IKEv2 のモビリティおよびマルチホーム プロトコル (MOBIKE)

IKEv2 のモビリティおよびマルチホーム プロトコル (MOBIKE) には VPN セッションを維持する機能があり、ユーザが別の IP アドレスに移動してもゲートウェイとの IKE セキュリティ アソシエーションを再確立する必要がありません。例えば、ユーザはオフィス内で固定のイーサネット接続を使用中に VPN トンネルを確立できます。MOBIKE を利用すると、ユーザはノートパソコンの接続を切断して VPN セッションを中断することなくオフィスの無線 LAN に移行できます。

MOBIKE の動作は透過的であり、管理者が追加で設定を行ったり、ユーザが考慮したりする必要はありません。

IPsec (フェーズ 2) プロポーザルについて

IPsec (フェーズ 2) プロポーザルは、IKEv1 と IKEv2 の両方で発生します。このフェーズでは、通信する双方の間で、使用するセキュリティ種別、トンネル通過トラフィックの暗号化方式 (必要な場合)、および鍵再設定までのトンネル存続期間がネゴシエートされます。

個々のパケット用のセキュリティには、次の 2 種類があります。

- 「**カプセル化セキュリティ ペイロード (ESP)**」- 各パケットのデータ部を、通信相手間でネゴシエートされたプロトコルを使用して暗号化します。
- 「**認証ヘッダー (AH)**」- 各パケットの認証ヘッダーには認証情報が含まれています。これにより、情報の信憑性が保証されるとともに、改ざんが防止されます。AH のデータには暗号化は一切使用されません。

SonicOS は、VPN 経由のトラフィックに対して、次の**暗号化**方式をサポートしています。

- DES
- 3DES
- なし
- AES-128
- AES-192
- AES-256
- AESGCM16-128
- AESGCM16-192
- AESGCM16-256
- AESGMAC-128
- AESGMAC-192
- AESGMAC-256

SonicOS は、次の**認証**方式をサポートしています。

- MD5
- SHA1
- SHA256
- SHA384
- SHA512
- AES-XCBC
- なし

Suite B 暗号化について

SonicOS は、Suite B 暗号化をサポートします。Suite B とは、米国家安全保障局 (NSA) が Cryptographic Modernization Program (暗号近代化プログラム) の一環として規定する暗号化アルゴリズム群です。機密情報と非機密情報の両方に対する相互運用可能な暗号ベースとして機能します。Suite B 暗号化は、米国立標準技術研究所 (NIST) によって米政府での使用が承認されています。

Suite B のほとんどのコンポーネントは、FIPS 規格から採用されています。

- 鍵サイズが 128 ビットから 256 ビットまでの AES (Advanced Encryption Standard: 拡張暗号化規格) (SECRET レベルまでの機密情報に対する十分な保護を提供します)。
- ECDSA (Elliptic Curve Digital Signature Algorithm: 楕円曲線デジタル署名アルゴリズム) - デジタル署名 (SECRET レベルまでの機密情報に対する十分な保護を提供します)。
- ECDH (Elliptic Curve Diffie Hellman: 楕円曲線ディフィーヘルマン) - 鍵合意 (SECRET レベルまでの機密情報に対する十分な保護を提供します)。
- Secure Hash Algorithm 2 (SHA256、SHA384、SHA512) - メッセージ ダイジェスト (TOP SECRET レベルまでの機密情報に対する十分な保護を提供します)。

VPN ベースの設定と表示

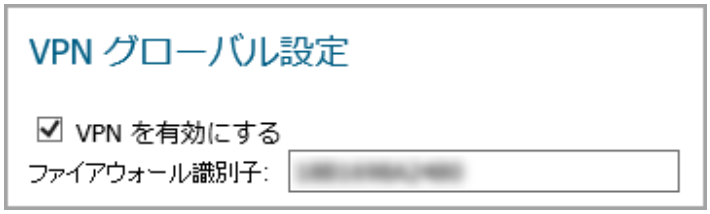
VPN ページは、選択されたオプションに応じて、一連のテーブルと設定を提供します。テーブルと設定の閲覧方法については、『*SonicOS 6.5 SonicOS について*管理ガイド』を参照してください。

「**VPN > 基本設定**」ページの詳細については、以下を参照してください。

- VPN グローバル設定
- VPN ポリシー
- 現在アクティブな VPN トンネル

「VPN > 基本設定」ページ

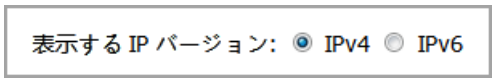
VPN グローバル設定



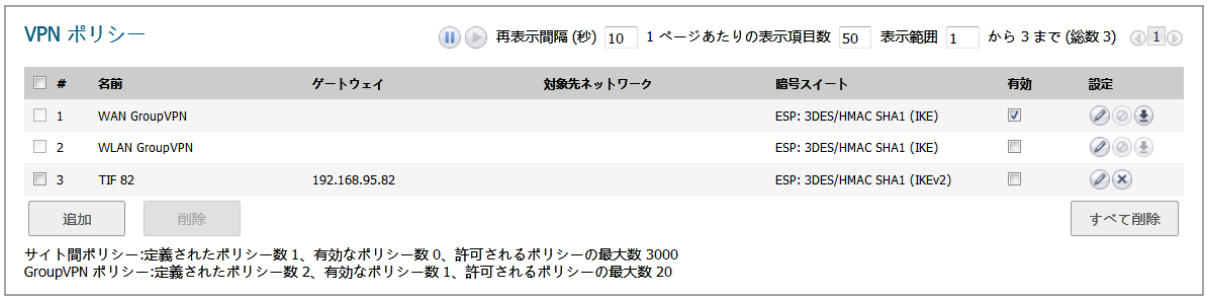
「**VPN > 基本設定**」ページの「**グローバル VPN 設定**」セクションには、次の情報が表示されます。

VPN を有効にする	SonicWall® セキュリティ ポリシーを通じて VPN ポリシーを有効にする場合に選択します。
ファイアウォール識別子	VPN トンネルを設定する際に、この SonicWall 装置を指定します。既定値は装置のシリアル番号です。何か意味のある適当な名前に変更してもかまいません。
表示する IP バージョン	IP バージョン表示を設定します。**IPv4** または **IPv6** を指定できます。

SonicWall VPN は、IPv4 と IPv6 を両方サポートします (インターネットプロトコルバージョン 4 およびインターネットプロトコルバージョン 6)ウィンドウの右上にある変更したいものを選択することによって、2 つのバージョンを切り替えることができます。既定値表示は IPv4 です。



VPN ポリシー



すべての定義済 VPN ポリシーは、「**VPN ポリシー**」テーブルに表示されます。各エントリに表示される情報は以下のとおりです。

- 「**名前**」- 既定の名前またはユーザ定義の VPN ポリシー名。
- 「**ゲートウェイ**」- リモート ファイアウォールの IP アドレス。ワイルドカード IP アドレス 0.0.0.0 を使用している場合は、それが IP アドレスとして表示されます。
- 「**対象先ネットワーク**」- 対象先ネットワークの IP アドレス。
- 「**暗号スイート**」- VPN ポリシーで使われる暗号化の種類。
- 「**有効**」- ポリシーが有効かどうか。チェック ボックスをオンにすると、VPN ポリシーが有効になります。チェック ボックスをオフにすると、VPN ポリシーが無効になります。
- 「**設定**」- 個々の VPN ポリシーの管理オプションです。
  - **編集**アイコンを選択すると、VPN ポリシーを編集できます。

- **削除**アイコンはその行のポリシーを削除します。事前に定義されている GroupVPN ポリシーは削除できないため、**削除**アイコンが淡色表示になっています。
- **エクスポート**アイコンを選択すると、VPN ポリシーの設定がファイルとしてエクスポートされます。SonicWall グローバル VPN クライアントは、このファイルをローカルのインストールに使います。

「VPN ポリシー」テーブルの下には以下のボタンがあります。

追加	サイト間 VPN ポリシーを設定するには「**VPN ポリシー**」ウィンドウにアクセスします。
削除	選択されたものを削除します (削除する対象を指定するには、**名前**列内の VPN ポリシー名の前にあるチェック ボックスを先にオンにします)。GroupVPN ポリシーは削除できません。
すべて削除	「VPN ポリシー」テーブル内の VPN ポリシー (既定の VPN ポリシー以外) をすべて削除します。

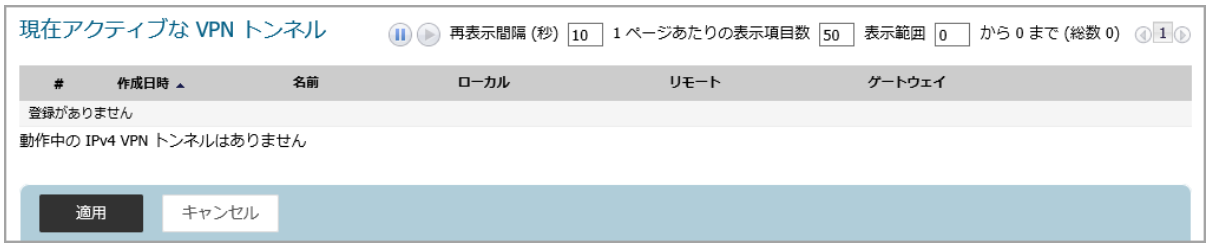
このテーブルの下には、サイト間 VPN ポリシーと GroupVPN ポリシーの両方について、VPN ポリシーに関する以下の統計値も示されます。

- 定義されたポリシー数
- 有効なポリシー数
- 許可されるポリシーの最大数

GroupVPN ポリシーは、ゾーンごとに最大 4 つまで定義できます。「**VPN ポリシー**」テーブルに、既定でこれらの GroupVPN ポリシー (**WAN GroupVPN**、**LAN GroupVPN**、**DMZ GroupVPN**、**WLAN GroupVPN**) がリストされます。GroupVPN の「**設定**」列で「**編集**」アイコンをクリックすると、GroupVPN ポリシーを設定するための「**セキュリティ ポリシー**」ウィンドウが表示されます。

メモ：VPN ポリシーは、VPN ゲートウェイ IP が同じである場合は、2 つの異なる WAN インターフェースを持つことはできません。

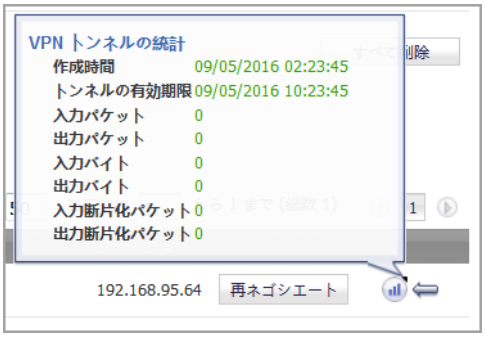
現在アクティブな VPN トンネル



現在アクティブな VPN トンネルのリストがこのセクションに表示されます。**「現在アクティブな VPN トンネル数」** テーブルには、各トンネルに関する以下の情報が表示されます。

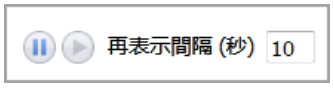
作成日時	トンネルが生成された日付と時間
名前	VPN ポリシーの名前
ローカル	トンネルのローカル LAN の IP アドレス
リモート	リモート対象先ネットワークの IP アドレス
ゲートウェイ	ピア ゲートウェイの IP アドレス

再ネゴシエートボタン	選択すると、VPN クライアントに強制的に VPN トンネルを再ネゴシエートさせます
統計アイコン	マウスカーソルを **統計** アイコンの上に置くと、**VPN トンネル統計** が表示されます。



左矢印アイコン	**左矢印** アイコンの上にマウスカーソルを置くと、関連する VPN ポリシーが「**VPN ポリシー**」テーブルの中央に表示されます

「**VPN ポリシー**」および「**現在アクティブな VPN トンネル**」テーブルの上部にある「**再表示間隔**」オプションを使用することにより、アクティブなトンネルを再表示することができます。



「**再表示間隔**」には、トンネルの再表示をどの程度の頻度で行うかを秒単位で指定します。「**一時停止**」アイコンを選択すると再表示が一時停止し、「**開始**」アイコンを選択すると再表示が開始されます。

IPv6 VPN の設定

IPv6 のサイト間 VPN は、「**VPN > 基本設定**」ページにある「**表示する IP バージョン**」ラジオ ボタンで「**IPv6**」オプションを選択した後、IPv4 VPN と同様の方法で設定できます。

現在 IPv6 でサポートされていない特定の VPN 機能があります。

- IKEv1 はサポートされません。
- GroupVPN はサポートされていません。
- トンネル インターフェースのルートベース VPN はサポートされていません。
- VPN を越えた DHCP はサポートされていません。
- L2TP サーバはサポートされていません。

IPv6 VPN ポリシーを設定する場合:

- 「**一般**」画面
  - 「**ゲートウェイ**」は、IPv6 アドレスを使用して設定する必要があります。FQDN はサポートされていません。
  - 「**IKE 認証**」の設定では、ローカルおよびピアの IKE ID に IPv6 アドレスを使用できます。
- 「**ネットワーク**」画面

- 「**ローカル ネットワーク**」および「**リモート ネットワーク**」には、IPv6 アドレス オブジェクト (または IPv6 アドレス オブジェクトを含むアドレス グループ) を選択する必要があります。
- **VPN を越えた DHCP** はサポートされていません。そのため、保護されたネットワーク用の DHCP オプションは使用できません。
- 「**ローカル ネットワーク**」の「**すべてのアドレス**」と、「**リモート ネットワーク**」の「**強制トンネル**」オプションは廃止されました。ただし、***すべて0*** の IPv6 ネットワーク アドレス オブジェクトを同じ機能や動作に対して選択できます。

- 「**プロポーザル**」画面では、**IKEv2 モード**のみがサポートされています。
- 「**詳細**」画面では、IPv6 VPN ポリシーのいくつかのオプションが無効になっています。
  - 「**この VPN ポリシーに対してアクセス ルールを自動生成しない**」は無効
  - 「**Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする**」は無効
  - 「**マルチキャストを有効にする**」は無効
  - 「**NAT ポリシーを適用する**」は無効

メモ：インターフェースは複数の IPv6 アドレスを持つことができるので、トンネルのローカル アドレスは定期的に変化することがあります。ユーザが一貫性のある IP アドレスを必要としている場合は、「**VPN ポリシーの適用先**」オプションとしてゾーンではなくインターフェースを設定し、アドレスを手動で指定します。このアドレスは、そのインターフェースに対する IPv6 アドレスの 1 つでなければなりません。

VPN が自動的に追加するルール コントロール

VPN ポリシーを追加すると、SonicOS は編集不可のアクセス ルールを自動作成し、トラフィックが適切なゾーンを通過することを許可します。「ローカル ネットワーク」に「Firewalled Subnets」が設定 (このケースでは LAN および DMS で構成) されて、ネットワークにサブネット `192.168.169.0` が設定されるという状況で、以下の VPN ポリシーについて検討してみましょう。

アクセス ルールの自動作成は一般的には非常に便利ですが、場合によっては VPN ポリシーをサポートするうえで自動作成の抑止が必要になります。例えば、大規模なハブアンドスポーク型 VPN (スポーク サイト全体が、簡単にスーパーネット化できるアドレス空間を使用したアドレスである) などです。ここで、2,000 のリモート サイトそれぞれにおけるハブ サイトでの LAN および DMZ アクセスを1 つのサブネットで提供する場合、アドレスは以下のようになります。

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

これらの各リモートサイト用に VPN ポリシーを作成した場合は 2,000 の VPN ポリシーが必要となり、8,000 のアクセス ルールも作成されます (各サイトに対して LAN -> VPN、DMZ -> VPN、VPN -> LAN、および VPN -> DMZ)。ただし、これらのアクセス ルールは、リモート サイトのスーパーネット化つまりアドレス範囲表現に対する 4 つのアクセス ルールですべて簡単に処理することができます (さらに具体的な許可または拒否のアクセス ルールを必要に応じて追加できます)。

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) または
remoteRange=Range 10.0.0.0-10.7.207.255

このレベルの集約を有効にするため、「**VPN ポリシー**」ダイアログの「**詳細**」タブに、サイト間 VPN ポリシーに関して「**この VPN ポリシーに対してアクセス ルールを自動生成しない**」オプションが用意されています。既定では、このチェックボックスがオフになっており、付随するアクセス ルールが自動的に作成されます。VPN ポリシーの作成時にこのチェックボックスをオンにすることにより、VPN トラフィックの個別アクセス ルールを作成できます。

2

サイト間 VPN

SonicWall VPN は、業界標準の IPsec VPN 実装に基づいています。モバイル ユーザ、在宅勤務者、リモート オフィス、およびパートナーをインターネット経由で接続するための、設定が簡単で安全なソリューションを提供します。モバイル ユーザ、在宅勤務者、およびブロードバンド (DSL またはケーブル) またはダイアルアップ インターネット アクセスを使用する他のリモート ユーザは、お使いのファイアウォールの SonicWall グローバル VPN クライアントおよび GroupVPN により、ネットワーク リソースに安全かつ簡単にアクセスできます。リモート オフィス ネットワークは、ネットワーク間 VPN 接続を有効にするサイト間 VPN 接続を使用して、お使いのネットワークに安全に接続することができます。

追加できるポリシーの最大数はお使いの SonicWall モデルによって異なります。より大型のモデルではより多くの接続が可能です。

メモ：リモート ユーザに対して、ネットワーク リソースへのアクセスを明示的に付与する必要があります。詳細については、*SonicOS 6.5 システム設定*を参照してください。アクセスの定義方法に応じて、GVC を使用して GroupVPN に接続するリモート クライアントだけでなく、NetExtender や SSL VPN 仮想オフィス ブックマークを使用してネットワーク リソースにアクセスするリモート ユーザに対しても影響を与えることができます。GVC、NetExtender または仮想オフィスのユーザがネットワーク リソースへアクセスすることを許可するには、ネットワーク アドレス オブジェクトかグループを、「**VPN アクセス**」 タブの許可リストに追加する必要があります。このウィンドウにアクセスするには、「**管理**」表示を選択して「**システム セットアップ**」で「**ユーザ > ローカル ユーザとグループ > ローカルユーザ > 追加 > VPN アクセス**」をクリックします。

このセクションでは、GroupVPN を含むサイト間ポリシーについて説明します。他のセクションでは、ルートベース VPN の自動プロビジョニングとトンネル インターフェース ポリシーについて説明します。この種のポリシーに対する設定の詳細については、以下のセクションに移動してください。

- VPN 自動プロビジョニング
- トンネル インターフェースルート ベース VPN

トピック:

- サイト間設定の計画
- 一般的な VPN 構成
- GroupVPN ポリシーの管理
- サイト間 VPN ポリシーの作成

サイト間設定の計画

サイト間 VPN を設定するときは多くの選択肢があります。例えば、次のような設定が可能です。

支社 (ゲートウェイ間)	SonicWall ファイアウォールが VPN トンネルを介して別の SonicWall ファイアウォールに接続するように設定されます。あるいは、SonicWall が IPSec を介して別のメーカーのファイアウォールに接続するように設定されます。
ハブとスポークの設計	すべての SonicWall VPN ゲートウェイが、企業のファイアウォールなど、中央のハブに接続されるように設計されます。ハブには静的な IP アドレスが必要ですが、スポークには動的な IP アドレスを持たせることができます。スポークが動的である場合、ハブは SonicWall ネットワーク セキュリティ装置でなければなりません。
メッシュ設計	すべてのサイトがすべての他のサイトに接続されます。すべてのサイトに静的な IP アドレスが必要です。

SonicWall では、これらの決定を支援する動画クリップとナレッジ ベース記事を用意しています。

ビデオ：サイト間 VPN の設定例を示す情報ビデオがオンラインで提供されています。例えば、「事前共有鍵を使用してメイン モードのサイト間 VPN を作成する方法」や「事前共有鍵を使用してアグレッシブ モードのサイト間 VPN を作成する方法」を参照してください。

その他のビデオは、以下でご覧いただけます。
https://www.sonicwall.com/ja-jp/support/video-tutorials

ヒント：サイト間 VPN に関する以下のナレッジ ベース記事を参照してください。

- *VPN: サイト間 VPN のシナリオと設定の種類 (SW12884)*
- *サイト間 VPN のトラブルシューティングに関する記事 (SW7570)*

VPN 接続の設計中には必ず、すべての適切な IP アドレッシング情報の文書を作成します。必要に応じてネットワーク ダイアグラムを作成し、参照用に使用します。その他注意すべき点は以下のとおりです。

- 動的であっても、静的であってもファイアウォールにはルーティングが可能な WAN IP アドレスが必要です。
- 動的および静的な IP アドレスを持つ VPN ネットワークでは、動的なアドレスを持つ VPN ゲートウェイで VPN 接続を開始する必要があります。

一般的な VPN 構成

このセクションでは、サイト間設定の一般的な手順を確認します。異なる特定のシナリオも可能で、そのいくつかは以下のセクションで説明します。IPv4 と IPv6 に対する IPsec VPN の設定は非常によく似ています。ただし、いくつかの特定の VPN 機能は、現在のところ IPv6 ではサポートされていません。詳細については、「IPv6 VPN の設定 (22 ページ)」を参照してください。

VPN を設定するには、以下の手順に従います。

1. 「**管理 | 接続性 | VPN > 基本設定**」ページに移動します。
2. 「**表示する IP バージョン**」フィールドで、**IPv4** または **IPv6** のうち適切なものを選択します。
3. 「**VPN ポリシー**」セクションで、「**追加**」を選択します。
4. 「**VPN ポリシー**」ダイアログの「**一般**」、「**ネットワーク**」、「**プロポーザル**」、「**詳細**」の各セクションで必要な設定を行ってください以下のセクションで、それらの個々のページに関する追加情報を提供します。

トピック:

- 「一般」画面での設定
- 「ネットワーク」画面での設定
- 「プロポーザル」画面での設定
- 「詳細」画面での設定

「一般」画面での設定

「**一般**」画面で、サイト間 VPN ポリシーの定義を開始します。IPv4 と IPv6 ネットワークで多少の違いがあり、注意が必要です。

IPv4 での VPN ポリシーの追加: 一般

1 IPv4 VPN を設定する場合、ドロップダウン メニューから「**ポリシー種別**」を選択します。

メモ:「**ポリシー種別**」フィールドは、IPv6 では使用できません。

2 「**認証方式**」ドロップダウン リストから認証方式を選択します。「**一般**」画面の残りのフィールドは、選択したオプションに応じて変化します。使用できるオプションは次のとおりです。

IPv4	IPv6
手動鍵	手動鍵
IKE (事前共有鍵を使用) (既定)	IKE (事前共有鍵を使用) (既定)
IKE (サード パーティ証明書を使用)	IKE (サード パーティ証明書を使用)
SonicWall 自動プロビジョニング クライアント	
SonicWall 自動プロビジョニング サーバ	

3 ポリシーの**名前**を入力します。

4 「**プライマリ IPSec ゲートウェイ名またはアドレス**」で、ゲートウェイの名前またはアドレスを入力します。

5 「**セカンダリ IPSec ゲートウェイ名またはアドレス**」で、ゲートウェイの名前またはアドレスを入力します。

6 「**IKE 認証**」で、必要な認証情報を入力します。

メモ：IKE 認証の設定時には、ローカルおよびピアの IKE ID に IPv6 アドレスを使用できます。

「ネットワーク」画面での設定

「**ネットワーク**」画面で、サイト間 VPN ポリシーを構成するネットワークを定義します。

IPv4 での VPN ポリシーの追加: ネットワーク

VPN ポリシーの「**ネットワーク**」画面で、「**ローカル ネットワーク**」オプションと「**リモート ネットワーク**」オプションからそれぞれローカル ネットワークとリモート ネットワークを選択します。

IPv6 に対しては、ドロップダウン メニューが唯一の提供されるオプションであり、IPv6 で使用可能なアドレスオブジェクトだけがリストされます。DHCP はサポートされませんので、これらのオプションは表示されません。同様に、「**ローカル ネットワーク**」の「**すべてのアドレス**」オプションと、「**リモート ネットワーク**」の「**強制トンネル**」オプションは削除されています。すべて 0 の IPv6 ネットワーク アドレス オブジェクトを同じ機能や動作に対して選択できます。

IPv4 に対しては、追加のオプションが提供されます。「**ローカル ネットワーク**」で、「**ローカル ネットワークをリストより選択**」するか、「**すべてのアドレス**」を選択できます。「**すべてのアドレス**」を選択した場合、信頼するゾーンと VPN ゾーンの間に自動追加ルールが作成されます。

「**リモート ネットワーク**」の IPv4 では、以下のうち 1 つが選択できます。

- **この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する。**
- **対象先ネットワークをリストより選択**。リストされているものがない場合、新しいアドレス オブジェクトまたはアドレス グループを作成できます。
- **IKEv2 IP プールを使用する**。IKEv2 設定ペイロードをサポートするには、これを選択します。

「プロポーザル」画面での設定

「**プロポーザル**」画面では、VPN ポリシーのセキュリティ パラメータを定義します。ページは IPv4 と IPv6 で同じですが、選択に応じてオプションは変化します。IPv4 では IKEv1 と IKEv2 の両方のオプションが「**鍵交換モード**」フィールドにありますが、IPv6 では IKEv2 のみとなります。

「詳細」画面での設定

IPv4 と IPv6 の「**詳細**」画面は似ていますが、「詳細設定: オプション利用可能性」に示されているように、一部のオプションはどちらか一方でのみ使用できます。オプションは、選択した認証方式によっても異なります。

詳細設定: オプション利用可能性

オプション	IP バージョン	
	IPv4	IPv6
キープ アライブを有効にする	サポート	サポート
この VPN ポリシーに対してアクセス ルールを自動生成しない	サポート	-
IPsec アンチリプレイを無効にする	サポート	サポート
Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする	サポート	-
マルチキャストを有効にする	サポート	-
Suite B 互換アルゴリズムのみを表示する	サポート	サポート
NAT ポリシーを適用する	サポート	-
SonicPointN レイヤ 3 管理を許可する	サポート	サポート
プライマリ IP アドレスを使用する	-	サポート
ローカル ゲートウェイ IP アドレスを指定する	-	サポート

詳細設定: オプション利用可能性

オプション	IP バージョン	
	IPv4	IPv6
セカンダリ ゲートウェイを先制する	サポート	サポート
プライマリ ゲートウェイ検知間隔 (秒)	サポート	サポート
IKE SA ネゴシエーション中に、トリガー パケットを送信しない	サポート	サポート
ハッシュと URL 証明書種別を受け入れる	サポート	サポート
ハッシュと URL 証明書種別を送信する	サポート	サポート

メモ：インターフェースは複数の IPv6 アドレスを持つことができるので、トンネルのローカル アドレスは定期的に変化することがあります。一貫した IP アドレスを必要とするユーザがいる場合は、「**プライマリ IP アドレスを使用する**」と「**ローカル ゲートウェイ IP アドレスを指定する**」のどちらかのオプションを選択するか、VPN ポリシーをゾーンではなくインターフェースにバインドされるように設定してください。「**ローカル ゲートウェイ IP アドレスを指定する**」で、アドレスを手動で指定します。このアドレスは、そのインターフェースに対する IPv6 アドレスの 1 つでなければなりません。

IPv6 での VPN ポリシーの追加: 詳細

IPv4 での VPN ポリシーの追加: 詳細

GroupVPN ポリシーの管理

GroupVPN 機能は、グローバル VPN クライアント (GVC) の自動 VPN ポリシー プロビジョニングを提供します。SonicWall ネットワーク セキュリティ装置の GroupVPN 機能および GVC により、VPN の配備および管理が効率化されます。クライアント ポリシー プロビジョニング技術を使用することにより、GVC ユーザ用に VPN ポリシーを定義できます。このポリシー情報は、ファイアウォール (VPN ゲートウェイ) から GVC に自動的にダウンロードされるため、リモート ユーザは VPN 接続のプロビジョニングに時間と労力を費やす必要がありません。

GroupVPN ポリシーは、ファイアウォール管理者による複数のグローバル VPN クライアントの設定および配備に役立ちます。**GroupVPN** は、GVC にのみ利用可能です。XAUTH/RADIUS またはサード パーティ証明書を GroupVPN と組み合わせて使用することをお勧めします。ゾーンに対する GroupVPN ポリシーの作成方法に関する詳細については、*SonicOS 6.5 システム設定* を参照するか、「**システム セットアップ**」の「**管理**」ビューに移動して、「**ネットワーク > ゾーン > 追加**」を選択してください。

SonicOS では、WAN ゾーンおよび WLAN ゾーン用の 2 つの既定 GroupVPN ポリシーが用意されています。これらのゾーンは一般に信頼度が低いゾーンです。既定の GroupVPN ポリシー (以下の 2 つ) が「**VPN > 基本設定**」ページの「**VPN ポリシー**」テーブルに表示されます。これらはカスタマイズできます。

- WAN GroupVPN
- WLAN GroupVPN

メモ：工場出荷時の既定の設定の SonicOS 6.5.4 では、GroupVPN ポリシーは自動的に作成されません。ただし、以前のバージョンの SonicOS からアップグレードした装置では、これらのポリシーは変更されません。グループ VPN およびグローバル VPN クライアントについては、『*グループ VPN/グローバル VPN クライアントのシナリオと設定の種類* (SW7411)』を参照してください。

トピック:

- 事前共有鍵を使用する IKE の設定
- サード パーティ証明書を使用する IKE の設定
- GroupVPN クライアント ポリシーのエクスポート

事前共有鍵を使用する IKE の設定

事前共有鍵を使用する WAN GroupVPN を設定するには、次の手順に従います。

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 **WAN GroupVPN** ポリシーの**編集**アイコンを選択します。

「**一般設定**」画面において、**IKE (事前共有鍵を使用)** は「**認証方式**」の既定の設定です。「**共有鍵**」フィールドの共有鍵は、ファイアウォールによって自動的に生成されます。独自の事前共有鍵を生成することが可能です。独自に設定する共有鍵は、4 文字以上でなければなりません。

メモ：GroupVPN ポリシーの名前を変更することはできません。

3 「**プロポーザル**」を選択して設定手順を進めます。

4 「**IKE (フェーズ 1) プロポーザル**」セクションで、次の設定を選択します。

- 「**DH グループ**」ドロップダウン メニューの「**グループ 2**」 (既定値) を選択します。

  メモ：Windows XP L2TP クライアントは、DH グループ 2 でのみ動作します。

- 「**暗号化**」ドロップダウン メニューから、「**DES**」、「**3DES**」 (既定)、「**AES-128**」、「**AES-192**」、または「**AES-256**」を選択します。
- 「**認証**」ドロップダウン メニューから、使用する認証方式を選択します。選択肢は、「**MD5**」、「**SHA1**」 (既定)、「**SHA256**」、「**SHA384**」、または「**SHA512**」です。
- 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

5 「**IPSec (フェーズ 2) プロポーザル**」セクションで、次の設定を選択します。

- 「**プロトコル**」ドロップダウン メニューから、「**ESP**」 (既定) を選択します。
- 「**暗号化**」ドロップダウン メニューから、「**3DES**」 (既定)、「**AES-128**」、「**AES-192**」、または「**AES-256**」を選択します。
- 「**認証**」ドロップダウン メニューから、使用する認証方式を選択します。選択肢は、「**MD5**」、「**SHA1**」(既定)、「**SHA256**」、「**SHA384**」、「**SHA512**」、「**AES-XCBC**」、または「**なし**」です。
- 追加のセキュリティ層として Diffie-Helman 鍵交換を追加する場合は、「**Perfect Forward Secrecy を有効にする**」を選択します。
- 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

6 「**詳細設定**」を選択します。

7 GroupVPN ポリシーに適用する次のオプション設定をすべて選択します。

詳細設定

IPsec アンチリプレイを無効にする	重複したシーケンス番号を持つパケットが破棄されないようにします。
マルチキャストを有効にする	IP マルチキャスト トラフィック (音声 (VoIP など)/映像アプリケーション) が VPN トンネルを通過できるようにします。
クライアントに複数のプロポーザルを許可する	クライアント向けの複数のプロポーザル (IKE (フェーズ 1) プロポーザル、IKE (フェーズ 2) プロポーザルなど) を許可します。
IKE モード設定を有効にする	SonicOS が、内部 IP アドレス、DNS サーバ、または WINS サーバをサードパーティのクライアント (iOS 機器や Avaya IP 電話など) に割り当てることができるようにします。
この SA を経由しての管理:	- VPN ポリシーを使用してファイアウォールを管理する場合は、管理方法として「**HTTPS**」、「**SSH**」、または「**SNMP**」を選択します。 **メモ：**SSH は、IPv4 に対してのみ有効です。
デフォルト ゲートウェイ	この VPN ポリシーの受信 IPSec パケットに関して既定ネットワーク ルートの IP アドレスを指定できます。着信パケットはファイアウォールによってデコードされ、ファイアウォールで設定された静的ルートと比較されます。 パケットには任意の送信先 IP アドレスが含まれている可能性があるので、トラフィックを処理する十分な静的ルートを設定することはできません。IPSec トンネルを介して受信されるパケットでは、ファイアウォールによってルートが検出されます。ルートが検出されない場合、セキュリティ装置によってデフォルト ゲートウェイがチェックされます。デフォルト ゲートウェイが検出されると、パケットはゲートウェイを介してルーティングされます。そうでない場合、パケットは破棄されます。
XAUTH を利用した VPN クライアントの認証を要求する	この VPN トンネルの受信トラフィックがすべて認証済みのユーザからのものであることを要求します。認証されていないトラフィックは VPN トンネルでは許可されません。既定で「**Trusted Users**」グループが選択されています。「**XAUTH に使用するユーザ グループ**」メニューから、別のユーザ グループまたは「**Everyone**」を選択することができます。
認証されていない VPN クライアントのアクセス許可	認証されていない VPN クライアント アクセスを有効にすることができます。「**XAUTH を利用した VPN クライアントの認証を要求する**」をオフにすると、「**認証されていない VPN クライアントのアクセス許可**」メニューが有効になります。事前定義オプションのメニューからアドレス オブジェクトまたはアドレス グループを選択するか、「**アドレス オブジェクトの作成**」または「**アドレス グループの作成**」を選択して新規作成します。

8 「**クライアント**」を選択します。

9 次の中から GroupVPN ポリシーに適用したい設定をすべて選択します。

ユーザ名とパスワードのキャッシュ

XAUTH ユーザ名とパスワードのクライアント キャッシュ	グローバル VPN クライアントがユーザ名とパスワードをキャッシュできます。 • 「**無効**」が選択されると、ユーザ名とパスワードをグローバル VPN クライアントがキャッシュできないようにします。接続が有効なとき、IKE フェーズ 1 の鍵交換のたびにユーザはユーザ名とパスワードを要求されます。このオプションは既定の設定です。 • 「**セッション単位**」が選択されると、接続が無効化されるまでの間、接続を有効化してその確認が行われるたびにグローバル VPN クライアント ユーザがユーザ名とパスワードを要求されます。このユーザ名とパスワードは IKE フェーズ 1 の鍵交換で使用されます。 • 「**常に**」が選択されると、接続が有効化されたときに 1 回だけ、グローバル VPN クライアント ユーザがユーザ名とパスワードを要求されます。その際、ユーザ名とパスワードをキャッシュするかどうか問われます。

クライアント接続

仮想アダプターの設定	グローバル VPN クライアント (GVC) による仮想アダプタの使用は、仮想アダプタにアドレスを割り当てるため、DHCP サーバ、内部 SonicOS または指定された外部 DHCP サーバによって左右されます。 予測可能なアドレッシングが要件の 1 つとされるインスタンスでは、仮想アダプタの MAC アドレスを取得して、DHCP リース予約を作成しなければなりません。仮想アダプタのアドレッシングを提供する管理費用を削減するため、GroupVPN を設定して仮想アダプタの IP 設定の静的アドレッシングを許可できます。 **メモ**：この機能では、SonicWall GVC を使用する必要があります。 次のいずれかを選択します。 • この GroupVPN 接続で仮想アダプタを使わない場合は、「**なし**」を選択します。このオプションは既定の設定です。 • 「**DHCP リース**」を選択すると、仮想アダプタが、「**VPN > VPN を越えた DHCP**」ページの設定に従い、自分の IP 設定を DHCP サーバからのみ取得します。 • 「**DHCP リースまたは手動設定**」を選択すると、GVC がファイアウォールに接続した時に、ファイアウォールのポリシーは GVC が仮想アダプタを使用するよう指示しますが、仮想アダプタが手動で設定されている場合、DHCP メッセージは抑止されます。この設定値はファイアウォールによって記録されるので、手動で割り当てられた IP アドレスに対して ARP のプロキシが行えるようになります。設計により、現在は仮想アダプタの IP アドレスの割り当てには制限がありません。重複した静的アドレスのみが許可されていません。
コネクションの制御	各ゲートウェイの対象先ネットワークに一致しているクライアントネットワーク トラフィックは、そのゲートウェイの VPN トンネルを介して送信されます。次のいずれかを選択します。 • 「**このゲートウェイのみ**」一度に 1 つの接続を有効にできます。ゲートウェイのポリシーで指定されているように対象先ネットワークに一致するトラフィックは VPN トンネルを介して送信されます。 このオプションを「**このゲートウェイをデフォルト ルートに設定する**」とともに選択する場合、インターネット トラフィックも VPN トンネルを介して送信されます。「**このゲートウェイをデフォルト ルートに設定する**」を選択しないと、インターネット トラフィックは遮断されます。 • 「**すべてのゲートウェイ**」同時に 1 つ以上の接続を有効にできます。各ゲートウェイの対象先ネットワークに一致しているトラフィックは特定のゲートウェイの VPN トンネルを介して送信されます。 このオプションを「**このゲートウェイをデフォルト ルートに設定する**」とともに選択する場合、インターネット トラフィックも VPN トンネルを介して送信されます。 このオプションを選択して、なおかつ「**このゲートウェイをデフォルト ルートに設定する**」は選択しない場合、インターネット トラフィックは遮断されます。複数のゲートウェイのうちいずれか 1 つのみ、「**このゲートウェイをデフォルト ルートに設定する**」を有効化できます。 • 「**トンネルを分割する**」VPN ユーザはローカル インターネット接続と VPN 接続の両方が可能です。このオプションは既定の設定です。

このゲートウェイをデフォルト ルートに設定する	すべてのリモート VPN 接続が VPN トンネル経由でインターネットにアクセスするとき、このチェック ボックスをオンにします。このオプションを使用する場合は、VPN ポリシーを 1 つだけ設定できます。既定では、このオプションはオフになっています。
VPN アクセス制御リストを適用する	VPN アクセス制御リストを適用するとき、このチェック ボックスをオンにします。これをオンにすると、指定されたユーザは、そのユーザのために設定されたネットワークだけにアクセスできるようになります (詳細は、*SonicOS 6.5 システム設定* の**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** を参照してください)。このオプションは既定では無効になっています。
クライアントへの初期プロビジョニング	
シンプル クライアント プロビジョニングに既定の鍵を使用する	ゲートウェイとの最初の交換でアグレッシブ モードが使用され、VPN クライアントでは既定の事前共有鍵が認証に使用されます。このオプションは既定では無効になっています。

10 「**OK**」を選択します。

11 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

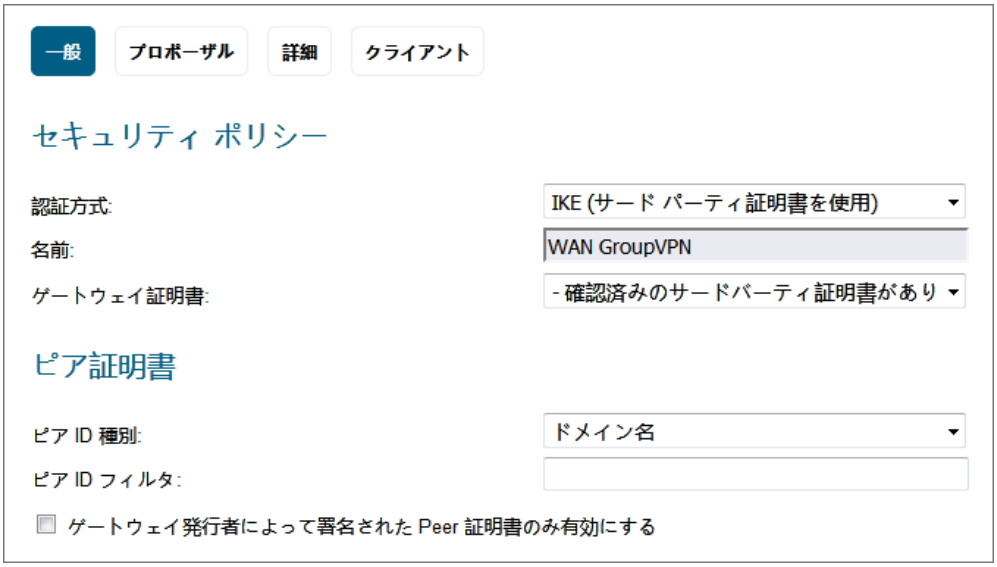
サード パーティ証明書を使用する IKE の設定

重要：サードパーティ証明書を使用して IKE で GroupVPN を設定する前に、証明書をファイアウォールにインストールする必要があります。

IKE (サードパーティ証明書) で GroupVPN を設定するには

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 **WAN GroupVPN** ポリシーの**編集**アイコンを選択します。



3 「**セキュリティ ポリシー**」セクションで、「**認証方式**」ドロップダウン メニューから「**IKE (サードパーティ証明書を使用)**」を選択します。

メモ：VPN ポリシー名は、既定で「WAN GroupVPN」となっており、変更できません。

4 「**ゲートウェイ証明書**」ドロップダウン メニューからファイアウォールの証明書を選択します。

この手順を開始する前にサードパーティ証明書をダウンロードしていない場合、「**ゲートウェイ証明書**」フィールドには、「**-確認済みのサードパーティ証明書がありません-**」と表示されます。

5 「**ピア 証明書**」セクションでは、「**ピア ID 種別**」ドロップダウン メニューから次のピア ID 種別のいずれかを選択します。

識別名	これは証明書の「サブジェクト識別名」フィールド (既定では、すべての証明書に含まれ、発行元の認証局が設定する) に基づいています。 「サブジェクト識別名」の形式は、発行元の認証局によって決定されます。一般的なフィールドは、国 (C=)、組織 (O=)、組織の単位 (OU=)、一般名 (CN=)、住所 (L=) などですが、発行元の認証局ごとに異なります。実際の X509 証明書の「サブジェクト識別名」フィールドはバイナリ オブジェクトであるため、目的に応じて文字列に変換する必要があります。フィールドは、次の例のようにフォワード スラッシュで区切られます。 `/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub` 最大で 3 つの組織の単位を追加できます。使用方法は、`c=*;o=*;ou=*;ou=*;ou=*;cn=*` です。最後のエントリにはセミコロンは不要です。*c=us* のように少なくとも 1 つのエントリを入力する必要があります。
電子メール ID **ドメイン ID**	「**電子メール ID**」と「**ドメイン ID**」は、証明書の「サブジェクト代替名」フィールド (すべての証明書に既定では含まれていない) に基づいています。証明書に「サブジェクト代替名」フィールドが含まれていない場合、このフィルタは機能しません。

6 「**ピア ID フィルタ**」フィールドにピア ID フィルタを入力します。

「**電子メール**」と「**ドメイン名**」フィルタには、要求される許容範囲を識別する文字列または部分文字列が含まれている可能性があります。入力した文字列には大文字と小文字の区別がなく、ワイルド カード文字 `*` (2 文字以上の場合) および `?` (1 文字の場合) を含めることができます。例えば、「**電子メール**」が選択されているときに文字列が `*@sonicwall.com` である場合、`@sonicwall.com` で終わる電子メール アドレスを持つユーザがアクセスでき、**ドメイン名**が選択されているときに文字列 `*sv.us.sonicwall.com` である場合、`sv.us.sonicwall.com` で終わるドメイン名を持つユーザがアクセスできます。

7 「**ゲートウェイ発行者によって署名された Peer 証明書のみ有効にする**」をオンにして、ピア証明書が「**ゲートウェイ証明書**」メニューで指定された発行者によって署名されていなければならないことを指定します。

8 「**プロポーザル**」を選択します。

9 「**IKE (フェーズ 1)**」セクションで、次の設定を選択します。

a 「**DH グループ**」で、「**グループ 1**」、「**グループ 2**」(既定)、「**グループ 5**」、または「**グループ 14**」を選択します。

> **メモ**：Windows XP L2TP クライアントは、DH グループ 2 でのみ動作します。

b 「**暗号化**」で、「**DES**」、「**3DES**」(既定)、「**AES-128**」、「**AES-192**」、または「**AES-256**」を選択します。

c 「**認証**」で、使用する認証方式を選択します。選択肢は、「**MD5**」、「**SHA1**」(既定)、「**SHA256**」、「**SHA384**」、「**SHA512**」、「**AES-XCBC**」、または「**なし**」です。

d 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

10 「**IPSec (フェーズ 2)**」セクションで、次の設定を選択します。

a 「**プロトコル**」で、「**ESP**」(既定) を選択します。

b 「**暗号化**」で、「**3DES**」(既定)、「**AES-128**」、「**AES-192**」、または「**AES-256**」を選択します。

c 「**認証**」で、使用する認証方式を選択します。選択肢は、「**MD5**」、「**SHA1**」(既定)、「**SHA256**」、「**SHA384**」、「**SHA512**」、「**AES-XCBC**」、または「**なし**」です。

d セキュリティをさらに強化するために Diffie-Helman 鍵交換を追加する場合は、「**Perfect Forward Secrecy を有効にする**」を選択します。

e 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

11 「**詳細設定**」を選択します。

12 以下のオプション設定のうち GroupVPN ポリシーに設定したいものをすべて選択します。

IPsec アンチリプレイを無効にする	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。
マルチキャストを有効にする	IP マルチキャスト トラフィック (音声 (VoIP など)/映像アプリケーション) が VPN トンネルを通過できるようにします。
クライアントに複数のプロポーザルを許可する	クライアント向けの複数のプロポーザル (IKE (フェーズ 1) プロポーザル、IKE (フェーズ 2) プロポーザルなど) を許可します。
IKE モード設定を有効にする	SonicOS は内部 IP アドレス、DNS サーバ、または WINS サーバを、iOS 機器や Avaya IP フォンのようなサードパーティ クライアントに割り当てることができます。
この SA を経由しての管理	VPN ポリシーを使用してファイアウォールを管理する場合は、管理方法として「**HTTPS**」、「**SSH**」、または「**SNMP**」を 1 つ以上選択します。 **メモ：**SSH は、IPv4 に対してのみ有効です。

デフォルト ゲートウェイ	**「この SA 経由ですべてのインターネット トラフィックが送られます」**チェック ボックスを使用してリモート サイトとともにセントラル サイトで使用します。「デフォルト LAN ゲートウェイ」を使用すると、この SA の受信 IPSec パケットに関して既定 LAN ルートの IP アドレスを指定できます。 着信パケットはファイアウォールによってデコードされ、ファイアウォールで設定された静的ルートと比較されます。パケットには任意の送信先 IP アドレスが含まれている可能性があるので、トラフィックを処理する十分な静的ルートを設定することはできません。IPSec トンネルを介して受信されるパケットでは、ファイアウォールによってLAN のルートが検出されます。ルートが検出されない場合、ファイアウォールによってデフォルトLAN ゲートウェイがチェックされます。デフォルト LAN ゲートウェイが検出されると、パケットはゲートウェイを介してルーティングされます。そうでない場合、パケットは破棄されます。
OCSP 確認を有効にする と OCSP 確認用 URL	VPN 証明書状況を確認する OCSP (Online Certificate Status Protocol) の使用を有効にし、証明書状況を確認する URL を指定します。
XAUTH を利用した VPN クライアントの認証を要求する	この VPN ポリシーの受信トラフィックがすべて認証済みのユーザからのものであることが要求されます。認証されていないトラフィックは VPN トンネルでは許可されません。
XAUTH に使用するユーザ グループ	認証用に定義済みユーザ グループを選択できます。
認証されていない VPN クライアントのアクセス許可	認証されていないグローバル VPN クライアント アクセスのネットワーク セグメントを指定できます。

13 「**クライアント**」を選択します。

14 次のボックスのうちグローバル VPN クライアント プロビジョニングに適用したいものをすべて選択します。

XAUTH ユーザ名とパスワードのキャッシュ	グローバル VPN クライアントがユーザ名とパスワードをキャッシュできます。 • 「**無効**」を選択すると、グローバル VPN クライアントはユーザ名とパスワードをキャッシュすることが禁止されます。接続が有効である場合、IKE フェーズ 1 の再入力があるたびに、ユーザはユーザ名とパスワードを要求されます。 • 「**セッション単位**」を選択すると、ユーザは接続有効化時に毎回ユーザ名とパスワード (接続が無効になるまで有効) を要求されます。このユーザ名とパスワードは IKE フェーズ 1 の再入力で使用されます。 • 「**常に有効**」を選択すると、ユーザは接続有効化時に 1 回だけユーザ名とパスワードを要求されます。その際、ユーザ名とパスワードをキャッシュするかどうか問われます。
仮想アダプターの設定	グローバル VPN クライアント (GVC) による仮想アダプタの使用は、仮想アダプタにアドレスを割り当てるため、DHCP サーバ、内部 SonicOS または指定された外部 DHCP サーバによって左右されます。 予測可能なアドレッシングが要件の 1 つとされるインスタンスでは、仮想アダプタの MAC アドレスを取得して、DHCP リース予約を作成しなければなりません。仮想アダプタのアドレッシングを提供する管理負荷を削減するため、GroupVPN を設定して仮想アダプタの IP 設定の静的アドレッシングを許可できます。この機能では、SonicWall GVC を使用する必要があります。 • 「**なし**」を選択すると、この GroupVPN 接続で仮想アダプタは使われません。 • 「**DHCP リース**」を選択すると、仮想アダプタは「**VPN > VPN を越えた DHCP**」ページの設定に従い、自分の IP 設定を DHCP サーバからのみ取得します。 • 「**DHCP リースまたは手動設定**」を選択すると、GVC がファイアウォールに接続した時に、ファイアウォールのポリシーは GVC が仮想アダプタを使用するよう指示しますが、仮想アダプタが手動で設定されている場合、DHCP メッセージは抑止されます。設定値はファイアウォールによって記録されるので、手動で割り当てられた IP アドレスのプロキシ ARP を取得できます。設計により、現在は仮想アダプタの IP アドレスの割り当てには制限がありません。重複した静的アドレスのみが許可されていません。

コネクションの制御	各ゲートウェイの対象先ネットワークに一致しているクライアント ネットワーク トラフィックは、そのゲートウェイの VPN トンネルを介して送信されます。以下のいずれかのオプションを選択します。 • 「**このゲートウェイのみ**」一度に 1 つの接続を有効にできます。ゲートウェイのポリシーで指定されているように対象先ネットワークに一致するトラフィックは VPN トンネルを介して送信されます。 このオプションを「**このゲートウェイをデフォルト ルートに設定する**」とともに選択する場合、インターネット トラフィックも VPN トンネルを介して送信されます。「**このゲートウェイをデフォルト ルートに設定する**」を選択しないと、インターネット トラフィックは遮断されます。 • 「**すべてのゲートウェイ**」同時に 1 つ以上の接続を有効にできます。各ゲートウェイの対象先ネットワークに一致しているトラフィックは特定のゲートウェイの VPN トンネルを介して送信されます。 このオプションを「**このゲートウェイをデフォルト ルートに設定する**」とともに選択する場合、インターネット トラフィックも VPN トンネルを介して送信されます。このオプションを選択して、なおかつ「**このゲートウェイをデフォルト ルートに設定する**」は選択しない場合、インターネット トラフィックは遮断されます。複数のゲートウェイのうちいずれか 1 つのみ、「**このゲートウェイをデフォルト ルートに設定する**」を有効化できます。 **メモ**：複数のゲートウェイのうちいずれか 1 つのみ、「**このゲートウェイをデフォルト ルートに設定する**」を有効化できます。 • 「**トンネルを分割する**」VPN ユーザはローカル インターネット接続と VPN 接続の両方が可能です。このオプションは既定の設定です。
このゲートウェイをデフォルト ルートに設定する	すべてのリモート VPN 接続がこの VPN トンネル経由でインターネットにアクセスする場合は、このチェック ボックスをオンにします。この設定を使用する場合は、SA を 1 つだけ設定できます。
VPN アクセス制御リストを適用する	アクセス制御リストでクライアント接続を制御するには、このオプションを有効にします。
シンプル クライアント プロビジョニングに既定の鍵を使用する	ゲートウェイとの最初の交換でアグレッシブ モードが使用され、VPN クライアントでは既定の事前共有鍵が認証に使用されます。

15 「**OK**」を選択します。

16 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

GroupVPN クライアント ポリシーのエクスポート

グローバル VPN クライアント用の設定を含むファイルを、エンド ユーザに提供することができます。単に、GroupVPN クライアント ポリシーをファイアウォールからエクスポートしてください。

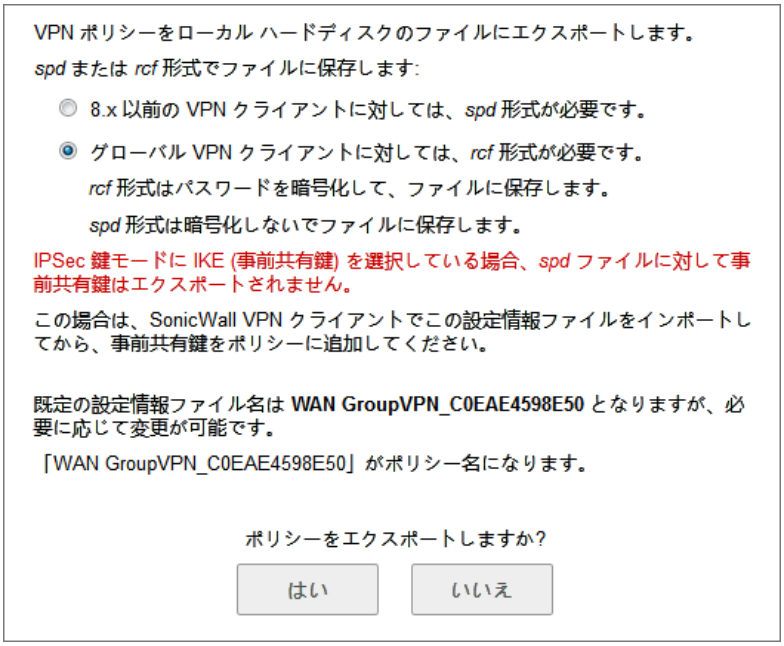
重要：設定ファイルをエクスポートするには、GroupVPN SA (Secure Association) をファイアウォールで有効にする必要があります。

グローバル VPN クライアント構成の設定をファイルにエクスポートするには、以下の手順に従います。

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 エクスポートする設定が有効になっていることを確認してください。

3 「**VPN ポリシー**」テーブルで、GroupVPN エントリの「**設定**」列にある**エクスポート**アイコンを選択します。



既定では「**グローバル VPN クライアントに対しては、rcf 形式が必要です。**」が選択されています。rcf 形式で保存されているファイルはパスワードを暗号化できます。ファイアウォールでは設定ファイル名に既定のファイル名が適用されますが、この名前は変更可能です。

4 「**はい**」を選択します。

5 「**エクスポートする対象先ネットワークを選択してください**」ドロップダウン リストから、「**VPN アクセス ネットワーク**」を選択します。

6 エクスポート ファイルを暗号化する場合は、パスワードを「**パスワード**」フィールドに入力し、「**パスワードの確認**」フィールドで再入力します。エクスポート ファイルを暗号化しない場合は、パスワードを入力する必要はありません。

7 「**適用**」を選択します。パスワードを入力しなかった場合は、選択を確認するメッセージが表示されます。

8 「**OK**」を選択します。設定ファイルを保存する前に変更することができます。

9 ファイルを保存します。

10 「**閉じる**」を選択します。

ファイルは保存するか、電気的にリモート ユーザに送信してグローバル VPN クライアントを設定することができます。

サイト間 VPN ポリシーの作成

サイト間 VPN により、複数の場所にある複数のオフィス相互の間に、公開ネットワークを通じて安全な接続を確立できます。それは企業のネットワークを拡張し、ある場所にあるコンピュータ リソースを、別の場所にいる従業員に利用可能にします。

既存のサイト間 VPN ポリシーを変更するか、新しく作成することができます。ポリシーを追加するには、「**VPN ポリシー**」テーブルの下にある「**追加**」をクリックします。既存のポリシーを変更するには、そのポリシーの「**編集**」アイコンをクリックします。サイト間 VPN の設定に際しては、以下のオプションが設定できます。

- 事前共有鍵を使用する設定
- マニュアル キーを使用する設定

- サードパーティ証明書を使った設定
- 「**SonicWall 自動プロビジョニング クライアント**」または「**SonicWall自動プロビジョニング サーバ**」これらのオプションについては、「VPN 自動プロビジョニング (73 ページ)」を参照してください。

このセクションでは、VPN トンネルが停止した場合にフェイルオーバーとして機能するようリモート SonicWall ファイアウォールを設定する方法、および静的ルートを設定する方法についても説明します。

- リモート SonicWall ネットワーク セキュリティ装置の設定
- 静的ルートへの VPN フェイルオーバーの設定.

ビデオ：サイト間 VPN の設定例を示す情報ビデオがオンラインで提供されています。例えば、「事前共有鍵を使用してメイン モードのサイト間 VPN を作成する方法」や「事前共有鍵を使用してアグレッシブ モードのサイト間 VPN を作成する方法」を参照してください。

その他のビデオは、以下でご覧いただけます。
https://www.sonicwall.com/ja-jp/support/video-tutorials。

事前共有鍵を使用する設定

事前共有鍵による IKE (インターネット鍵交換) を使用して VPN ポリシーを設定するには、次の手順を実行します。

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 「**追加**」を選択して新しいポリシーを作成するか、「**編集**」アイコンをクリックして既存のポリシーを更新します。

3 「**一般**」画面の「**ポリシー種別**」から「**サイト間**」を選択します。

4 「**認証方式**」から「**IKE (事前共有鍵を使用)**」を選択します。

5 ポリシーの名前を「**名前**」フィールドに入力します。

6 「**プライマリ IPSec ゲートウェイ名またはアドレス**」フィールドにリモート接続のホスト名または IP アドレスを入力します。

7 リモート VPN 機器が複数のエンドポイントをサポートしている場合は、リモート接続のセカンダリ ホスト名または IP アドレスを「**セカンダリ IPSec ゲートウェイ名またはアドレス**」フィールドに入力できます。(任意設定)

8 「**IKE 認証**」セクションで、「**事前共有鍵**」と「**事前共有鍵の確認**」フィールドに、共有鍵パスワードを入力します。これは、SA (セキュリティ アソシエーション) を設定するために使用します。共有鍵は文字と数字を組み合わせて 4 文字以上で、数字と文字を両方とも含んでいる必要があります。

9 両方のフィールドで共有鍵を表示する場合は、「**事前共有鍵を隠す**」チェックボックスをオフにします。既定では、「**事前共有鍵を隠す**」チェックボックスがオンになっており、共有鍵は黒い丸の列として表示されます。

10 必要に応じて、このポリシーの「**ローカル IKE ID**」および「**ピア IKE ID**」を指定します。

ドロップダウン メニューで、以下の ID から選択できます。

- **IPv4 アドレス**
- **ドメイン名**
- **電子メール アドレス**
- **ファイアウォール識別子**
- **鍵識別子**

既定では、「**IP アドレス**」 (ID_IPv4_ADDR) がメイン モード ネゴシエーションに使用され、ファイアウォール識別子 (ID_USER_FQDN) がアグレッシブ モードに使用されます。

11 「**ローカル IKE ID**」と「**ピア IKE ID**」フィールドに、アドレス、名前、または ID を入力します。

12 「**ネットワーク**」をクリックします。

13 「**ローカル ネットワーク**」の下で、次のいずれかを選択します。

ローカル ネットワークをリストより選択	特定のローカル ネットワークが VPN トンネルにアクセス可能である場合は、ドロップダウン メニューからローカル ネットワークを選択します。
すべてのアドレス	このオプションは、トラフィックがすべてのローカル ネットワークから発信できるか、ピアで「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」が選択されている場合に使用します。保護ゾーンと VPN ゾーンの間に、自動追加のルールが作成されます。 **メモ：**VPN を越えた DHCP は IKEv2 ではサポートされていません。

14 「**リモート ネットワーク**」の下で、次のいずれかを選択します。

この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する	ローカル ユーザからの暗号化されていないトラフィックを 装置から発信できないようにする場合は、このオプションを選択します。 **メモ：**この設定を使用する場合は、SA を 1 つだけ設定できます。
対象先ネットワークは、この VPN トンネルを通じた DHCP を使用して IP アドレスを取得する	リモート ネットワークがローカル ネットワークの DHCP サーバから IP アドレスを要求する場合、このオプションを選択します。 **メモ：**このオプションは、「**プロポーザル**」画面で「**メイン モード**」または「**アグレッシブ モード**」を選択した場合にのみ使用できます。
対象先ネットワークをリストより選択	ドロップダウン メニューからリモート ネットワークを選択します。
IKEv2 IP プールを使用する	IKEv2 設定ペイロードをサポートするには、このオプションを選択します。 **メモ：**このオプションは、「**プロポーザル**」画面で「**IKEv2 モード**」を選択した場合にのみ使用できます。

15 「**プロポーザル**」を選択します。

16 「**IKE (フェーズ 1) プロポーザル**」で、「**鍵交換モード**」ドロップダウン メニューから以下のオプションのうち 1 つを選択します。

メイン モード	IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
アグレッシブ モード	通常は WAN アドレッシングが動的に割り当てられる場合に使用されます。IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
IKEv2 モード	すべてのネゴシエーションを、IKEv1 フェーズ 1 よりも IKEv2 プロトコルで実行するようにします。 **メモ：IKE v2 モード**を選択する場合は、VPN トンネルの両端で IKE v2 を使用する必要があります。選択されると、「**DH グループ**」、「**暗号化**」、および「**認証**」フィールドは淡色表示となり、定義できなくなります。

17 「**IKE (フェーズ 1) プロポーザル**」の下の、残りのオプションの数値を設定します。「**DH グループ**」、「**暗号化**」、「**認証**」、および「**存続期間 (秒)**」の既定値はほとんどの VPN 設定に使用できます。

メモ：「**鍵交換モード**」フィールドにおいて「**IKEv2 モード**」が選択されている場合、「**DH グループ**」、「**暗号化**」、および「**認証**」フィールドは淡色表示となり、これらのオプションに対する選択はできません。

メモ：トンネルの反対側のフェーズ 1 の値が一致するように設定してください。

a 「**メイン モード**」または「**アグレッシブ モード**」の場合、「**DH グループ**」に対して、いくつかの Diffie Hellman 鍵交換から選択できます。

Suite B 暗号に含まれる Diffie Hellman グループ	その他の Diffie-Hellman オプション
256 ビット ランダム ECP グループ	グループ 1
384 ビット ランダム ECP グループ	グループ 2
521 ビット ランダム ECP グループ	グループ 5
192 ビット ランダム ECP グループ	グループ 14
224 ビット ランダム ECP グループ	

b 「**メイン モード**」または「**アグレッシブ モード**」を選択した場合は、「**暗号化**」フィールドに対して、「**3DES**」、「**DES**」、「**AES-128**」(既定)、「**AES-192**」、または「**AES-256**」のうちの 1 つをドロップダウン メニューから選択します。

c 「**メイン モード**」または「**アグレッシブ モード**」が選択されている場合、「**認証**」フィールドに対して、強化された認証セキュリティのために、「**SHA-1**」(既定)、「**MD5**」、「**SHA256**」、「**SHA384**」、または「**SHA512**」から選択してください。

d すべての「**鍵交換**」モードについて、「**存続期間 (秒)**」を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

18 「**IPsec (フェーズ 2) プロポーザル**」セクションで、オプションを設定します。「**プロトコル**」、「**暗号化**」、「**認証**」、「**Perfect Forward Secrecy を有効にする**」、および「**存続期間 (秒)**」の既定値は、ほとんどの VPN SA 設定に使用できます。

メモ：トンネルの反対側のフェーズ 2 の値が一致するように設定してください。

- 「**プロトコル**」フィールドで「**ESP**」を選択した場合は、「**暗号化**」フィールドで、Suite B 暗号化に含まれる以下の 6 つの暗号化アルゴリズムを選択できます。

Suite B 暗号化オプション	その他のオプション
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**なし**

- 「**プロトコル**」フィールドで「**AH**」を選択した場合、「**暗号化**」フィールドは淡色表示になり、オプションは選択できません。

19 「**詳細設定**」を選択します。

20 次のオプション設定のうち VPN ポリシーに適用したいものをすべて選択します。オプションは、「**プロポーザル**」画面でどのオプションを選択したかによって変わります。

オプション	メイン モードまたはアグレッシブ モード (下図「メイン モードとアグレッシブ モードの詳細設定」参照)	IKEv2 モード (下図「IKEv2 モードの詳細設定」参照)
詳細設定		
キープ アライブを有効にする	この VPN トンネルでピア間のハートビート メッセージを使用する場合に選択します。トンネルの一方の側が失敗した場合、キープアライブ ハートビートを使用することにより、両サイドが再び利用可能になったときにトンネルの自動的な再ネゴシエートが可能になります。 提案された存続期間が期限切れになるまで待つ必要はありません。 **メモ**：キープ アライブのオプションは、VPN ポリシーが VPN を越えた DHCP のセントラル ゲートウェイとして設定されている場合、または、プライマリ ゲートウェイ名またはアドレスが 0.0.0.0 である場合は、無効になります。	IKEv2 モードでは選択できません。
この VPN ポリシーに対してアクセス ルールを自動生成しない	*選択しない* (既定) と、付随するアクセス ルールが自動的に作成されます。詳細については、「VPN が自動的に追加するルール コントロール (23 ページ)」を参照してください。	*選択しない* (既定) と、付随するアクセス ルールが自動的に作成されます。詳細については、「VPN が自動的に追加するルール コントロール (23 ページ)」を参照してください。
IPsec アンチリプレイを無効にする	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。
XAUTH を利用した VPN クライアントの認証を要求する	この VPN ポリシーのすべての受信トラフィックは、XAUTH/RADIUS で認証されたユーザからのものである必要があります。認証されていないトラフィックは VPN トンネルでは許可されません。	IKEv2 モードでは使用できません。
Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。

オプション	メイン モードまたはアグレッシブ モード (下図「メイン モードとアグレッシブ モードの詳細設定」参照)	IKEv2 モード (下図「IKEv2 モードの詳細設定」参照)
マルチキャストを有効にする	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/ 映像アプリケーション) が VPN トンネルを通過できるようにします。	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/ 映像アプリケーション) が VPN トンネルを通過できるようにします。
WXA グループ	**なし** (既定値) または**グループ 1** を選択します。	**なし** (既定値) または**グループ 1** を選択します。
Suite B 互換アルゴリズムのみを表示する	Suite B 互換アルゴリズムのみを表示したい場合に選択します。	Suite B 互換アルゴリズムのみを表示したい場合に選択します。
NAT ポリシーを適用する	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。
SonicPointN レイヤ 3 管理を許可する	レイヤ 3 管理を許可したい場合に選択してください。	レイヤ 3 管理を許可したい場合に選択してください。
この SA を経由しての管理	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、このオプションで「**HTTPS**」、「**SSH**」、「**SNMP**」のいずれかを選択します。	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、このオプションで「**HTTPS**」、「**SSH**」、「**SNMP** 」のいずれかを選択します。
この SA を経由してのユーザ ログイン	「**HTTP**」または「**HTTPS**」、あるいは両方を選択すると、SA を使用してログインできます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。	「**HTTP**」または「**HTTPS**」、あるいは両方を選択すると、SA を使用してログインできます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。

オプション	メイン モードまたはアグレッシブ モード (下図「メイン モードとアグレッシブ モードの詳細設定」参照)	IKEv2 モード (下図「IKEv2 モードの詳細設定」参照)
デフォルト LAN ゲートウェイ (オプション)	トンネルに入る前の LAN を通じて未知のサブネットに向けたトラフィックをルーティングしたい場合、このオプションを選択してください。例えば、(「**ネットワーク**」画面の「**リモート ネットワーク**」で) 「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択した場合は、ルータのアドレスを入力してください。	トンネルに入る前の LAN を通じて未知のサブネットに向けたトラフィックをルーティングしたい場合、このオプションを選択してください。例えば、(「**ネットワーク**」画面の「**リモート ネットワーク**」で) 「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択した場合は、ルータのアドレスを入力してください。
VPN ポリシーの適用先	ドロップダウン リストからインターフェースかゾーンを選択します。WAN の負荷分散を使用していて、VPN でいずれかの WAN インターフェースを使用する場合は、ゾーン WAN が推奨される選択です。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。	ドロップダウン リストからインターフェースかゾーンを選択します。WAN の負荷分散を使用していて、VPN でいずれかの WAN インターフェースを使用する場合は、ゾーン WAN が推奨される選択です。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。
セカンダリ ゲートウェイを先制する	指定した時間の後に 2 番目のゲートウェイを先制 (プリエンプト) するには、このチェックボックスをオンにし、「**プライマリ ゲートウェイ検知間隔 (秒)**」オプションで目的の時間を設定します。既定の時間は 28800 秒、つまり 8 時間です。	指定した時間の後に 2 番目のゲートウェイを先制 (プリエンプト) するには、このチェックボックスをオンにし、「**プライマリ ゲートウェイ検知間隔 (秒)**」オプションで目的の時間を設定します。既定の時間は 28800 秒、つまり 8 時間です。
IKEv2 設定		
IKE SA ネゴシエーション中に、トリガー パケットを送信しない	メイン モードまたはアグレッシブ モードでは使用できません。	選択されてい「*ない*」 (既定)ピアがトリガー パケットを処理できない場合の相互運用性のために必要な場合のみ、オンにしてください。 セキュリティ ポリシー データベースから適切な保護 IP アドレス範囲を選択できるように IKEv2 応答側を支援するためにトリガー パケットを含めることをお勧めします。すべての実装でこの機能がサポートされているわけではないので、一部の IKE ピアでトリガー パケットを含めないようにしたほうがよいかもしれません。

オプション	メイン モードまたはアグレッシブ モード (下図「メイン モードとアグレッシブ モードの詳細設定」参照)	IKEv2 モード (下図「IKEv2 モードの詳細設定」参照)
ハッシュと URL 証明書種別を受け入れる	メイン モードまたはアグレッシブ モードでは使用できません。	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器に対して HTTP 証明書検索がサポートされているというメッセージを送信します。
ハッシュと URL 証明書種別を送信する	メイン モードまたはアグレッシブ モードでは使用できません。	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器からのメッセージに応答して、HTTP 証明書検索がサポートされているという内容を確認します。

メイン モードとアグレッシブ モードの詳細設定

IKEv2 モードの詳細設定

21 「**OK**」を選択します。

22 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

マニュアル キーを使用する設定

IPsec VPN トンネルを確立するための暗号化キーを手動で定義することができます。暗号化鍵または認証鍵の内容を指定する必要があるとき (例えば、VPN ピアの一方が特定の鍵を必要とするとき)、または暗号化と認証を無効にする必要があるとき、手動鍵を定義します。

手動鍵 (マニュアル キー) を使用した VPN ポリシーの設定

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 「**追加**」を選択して新しいポリシーを作成するか、「**編集**」アイコンを選択して既存のポリシーを更新します。

3 「**認証方式**」フィールドで、ドロップダウン メニューから「**マニュアル キー**」を選択します。ウィンドウに、マニュアル キーのオプションだけが表示されます。

4 ポリシーの名前を「**名前**」フィールドに入力します。

5 「**IPSec ゲートウェイ名またはアドレス**」フィールドにリモート接続のホスト名または IP アドレスを入力します。

6 「**ネットワーク**」をクリックします。

7 「**ローカル ネットワーク**」の下で、次のオプションのいずれかを選択します。

- 特定のローカル ネットワークが VPN トンネルにアクセス可能である場合は、「**ローカル ネットワークをリストより選択**」ドロップダウン メニューからローカル ネットワークを選択します。
- 任意のローカル ネットワークからトラフィックを発信できる場合は、「**すべてのアドレス**」を選択します。このオプションは、ピアで「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」が選択されている場合に使用します。保護ゾーンと VPN ゾーンの間に、自動追加のルールが作成されます。

8 「**リモートネットワーク**」の下で、次のいずれかを選択します。

- どのローカル ユーザによるトラフィックも暗号化されていなければファイアウォールから出られないようにするには、「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択します。

> **メモ**：この設定を使用する場合は、SA を 1 つだけ設定できます。

- あるいは、「**対象先ネットワークをリストから選択**」を選択して、アドレス オブジェクトまたはグループを選択します。

9 「**プロポーザル**」を選択します。

10 「**受信 SPI**」および「**送信 SPI**」を定義します。SPI (Security Parameter Index) は 16 進数で、長さは 3〜8 文字の範囲です。

重要：各 SA (Security Association) には一意の SPI が必要で、2 つの SA が同じ SPI を共有することはできません。ただし、各 SA の受信 SPI は送信 SPI と同一である可能性があります。

11 「**プロトコル**」、「**暗号化**」、および「**認証**」の既定値は、ほとんどの VPN SA 設定に使用できます。そぐわない場合には、ドロップダウン リストから値を選択してください。

メモ：「**プロトコル**」、「**暗号化**」、および「**認証**」の値は、リモート ファイアウォールの値と一致する必要があります。

- 「**プロトコル**」フィールドで「**ESP**」を選択した場合は、「**暗号化**」フィールドで、Suite B 暗号化に含まれる以下の 6 つの暗号化アルゴリズムを選択できます。
  - **DES**
  - **3DES**
  - **AES-128** (既定)
  - **AES-192**
  - **AES-256**
  - **なし**
- 「**プロトコル**」フィールドで「**AH**」を選択した場合、「**暗号化**」フィールドはグレー表示になり、オプションは選択できません。

12 「**暗号化鍵**」フィールドに 48 文字の 16 進数暗号化鍵を入力するか、既定値を使用します。この暗号キーはリモート SonicWall 暗号キーの設定に使用されるので、リモート ファイアウォールを設定するときに書き留めておいてください。

ヒント：有効な 16 進数の文字とは、0、1、2、3、4、5、6、7、8、9、a、b、c、d、e、および f です。例えば、1234567890abcdef は有効な DES または ARCFour 暗号キーの例です。不適切な暗号キーを入力すると、ブラウザ ウィンドウの下部にエラー メッセージが表示されます。

13 「**認証鍵**」フィールドに 40 文字の 16 進数認証鍵を入力するか、既定値を使用します。ファイアウォールの設定を指定するためにキーを書き留めます。

14 「**詳細設定**」を選択します。

15 GroupVPN ポリシーに適用する次のオプション設定をすべて選択します。

オプション	定義
この VPN ポリシーに対してアクセス ルールを自動生成しない	*選択しない* (既定) と、付随するアクセス ルールが自動的に作成されます。詳細については、「VPN が自動的に追加するルール コントロール (23 ページ)」を参照してください。
Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。
WXA グループ	**なし** (既定値) または**グループ 1** を選択します。
NAT ポリシーを適用する	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。 **ヒント**：インターフェースの設定例を紹介するビデオ チュートリアルがオンラインで公開されています。例えば、「重複ネットワークが存在するサイト間 VPN における NAT over VPN の設定方法」を参照してください。その他のビデオは、以下でご覧いただけます。 https://www.sonicwall.com/ja-jp/support/video-tutorials。

オプション	定義
SonicPointN レイヤ 3 管理を許可する	レイヤ 3 管理を許可したい場合に選択してください。
この SA を経由しての管理	ローカル SonicWall ファイアウォール を VPN トンネル経由で管理するには、「**HTTPS**」、「**SSH**」、「**SNMP**」、またはこの 3 つを組み合わせて選択します。
この SA を経由してのユーザ ログイン	「**HTTP**」、「**HTTPS**」、またはその両方を選択すると、SA を使用したログインがユーザに許可されます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。
デフォルト LAN ゲートウェイ (オプション)	トンネルに入る前の LAN を通じて未知のサブネットに向けたトラフィックをルーティングしたい場合、このオプションを選択してください。例えば、(「**ネットワーク**」画面の「**リモート ネットワーク**」で) 「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択した場合は、ルータのアドレスを入力してください。
VPN ポリシーの適用先	ドロップダウン リストからインターフェースかゾーンを選択します。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。

16 「**OK**」を選択します。

17 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

サードパーティ証明書を使った設定

メモ：サードパーティ証明書を使用した IKE で VPN ポリシーを設定する前に、サードパーティ証明書認定局からの有効な証明書を SonicWall にインストールしなくてはなりません。

SonicWall ファイアウォールでは、SonicWall 認証サービスの代わりに、サードパーティ証明書を認証に使うことも選択できます。サードパーティのプロバイダが提供する証明書やローカル証明書を使用するときは多くの手作業が生じます。そのため、デジタル証明書の主要な要素を理解する意味でも PKI (Public Key Infrastructure) の実装経験が必須です。

SonicWall は次の証明書プロバイダをサポートします。

- VeriSign
- Entrust

IKE およびサードパーティの証明書を使用して VPN SA を作成するには、次の手順に従います。

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 「**追加**」を選択して新しいポリシーを作成するか、「**編集**」アイコンを選択して既存のポリシーを更新します。

3 「**認証方式**」フィールドで、「**IKE (サード パーティ証明書を使用)** 」を選択します。「**VPN ポリシー**」ウィンドウの「**IKE 認証**」セクションに、サードパーティ証明書オプションが表示されます。

4 「**名前**」フィールドに SA 名を入力します。

5 「**プライマリ IPSec ゲートウェイ名またはアドレス**」フィールドにプライマリのリモート SonicWall の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。

6 セカンダリのリモート SonicWall がある場合、「**セカンダリ IPSec ゲートウェイ名またはアドレス**」フィールドにリモート対象先の IP アドレスまたは完全修飾ドメイン名を入力します。

7 「**IKE 認証**」で、「**ローカル証明書**」リストからサードパーティ証明書を選択します。このオプションを選択する前に、ローカル証明書をインポートする必要があります。

8 「**ローカル IKE ID 種別**」の既定値は「**証明書からの既定 ID**」です。または、次のいずれかを選択します。

- **識別名 (DN)**
- **電子メール ID (ユーザ FQDN)**
- **ドメイン名 (FQDN)**
- **IP アドレス (IPv4)**

これらの代替選択は、次のステップで説明する「**ピア IKE ID 種別**」の選択と同じです。

9 「**ピア IKE ID 種別**」メニューから次のピア ID 種別のいずれかを選択します。

ピア IKE ID 種別オプション	定義
証明書からの既定 ID	認証は、証明書の既定 ID から取られました。
識別名 (DN)	既定ですべての証明書に含まれている、証明書の「サブジェクト識別名」フィールドに基づいています。サイト間 VPN の場合は、完全な識別名を入力する必要があります。ワイルドカード文字はサポートされていません。 「サブジェクト識別名」の形式は、発行元の認証局によって決定されます。一般的なフィールドは、国 (C=)、組織 (O=)、組織の単位 (OU=)、一般名 (CN=)、住所 (L=) などですが、発行元の認証局ごとに異なります。実際の X509 証明書の「サブジェクト識別名」フィールドはバイナリオブジェクトであるため、目的に応じて文字列に変換する必要があります。フィールドは、次の例のようにフォワード スラッシュで区切られます。**/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**
電子メール ID (ユーザ FQDN)	**電子メール (UserFQDN)** に基づく認証種別は、既定ではすべての証明書に含まれて *いない* 証明書のサブジェクト代替名フィールドに基づいています。証明書に「サブジェクト代替名」が含まれている場合、その値を使用する必要があります。サイト間 VPN の場合、ワイルドカード文字は使用できません。電子メールの完全な値を入力する必要があります。Group VPN は複数のピアに接続することが想定されますが、サイト間 VPN は 1 つのピアに接続すると想定されるためです。
ドメイン名 (FQDN)	**ドメイン名 (UserFQDN)** に基づく認証種別は、既定ではすべての証明書に含まれて *いない* 証明書のサブジェクト代替名フィールドに基づいています。証明書に「サブジェクト代替名」が含まれている場合、その値を使用する必要があります。サイト間 VPN の場合、ワイルドカード文字は使用できません。ドメイン名の完全な値を入力する必要があります。グループ VPN は複数のピアに接続することが想定されますが、サイト間 VPN は 1 つのピアに接続すると想定されるためです。
IP アドレス (IPv4)	IPv4 IP アドレスに基づきます。

メモ：証明書の詳細 (サブジェクト代替名、識別名など) を参照するには、「**管理 | システム セットアップ | 装置 > 証明書**」ページに移動します。

10 「**ピア IKE ID**」フィールドに ID 文字列を入力します。

11 「**ネットワーク**」をクリックします。

12 「**ローカル ネットワーク**」の下で、次のオプションのいずれかを選択します。

- 特定のローカル ネットワークが VPN トンネルにアクセス可能である場合は、「**ローカル ネットワークをリストより選択**」ドロップダウン メニューからローカル ネットワークを選択します。
- 任意のローカル ネットワークからトラフィックを発信できる場合は、「**すべてのアドレス**」を選択します。このオプションは、ピアで「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」が選択されている場合に使用します。保護ゾーンと VPN ゾーンの間に、自動追加のルールが作成されます。

13 「**リモート ネットワーク**」で、次のオプションのいずれかを選択します。

- ローカル ユーザからの暗号化されていないトラフィックが から発信できない場合は、「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択します。

  メモ：この設定を使用する場合は、SA を 1 つだけ設定できます。

- あるいは、「**対象先ネットワークをリストから選択**」を選択して、アドレス オブジェクトまたはグループをドロップダウン リストから選択します。
- IKEv2 設定ペイロードをサポートして、アドレス オブジェクトまたは IP プール ネットワークをドロップダウン リストから選択したい場合、「**IKEv2 IP プールを使用する**」を選択します。

14 「**プロポーザル**」を選択します。

15 「**IKE (フェーズ 1) プロポーザル**」セクションで、次の設定を選択します。

メイン モード	IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
アグレッシブ モード	通常は WAN アドレッシングが動的に割り当てられる場合に使用されます。IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
IKEv2 モード	すべてのネゴシエーションを、IKEv1 のフレーズよりも IKEv2 プロトコルで実行するようにします。 **メモ：IKE v2 モード**を選択する場合は、VPN トンネルの両端で IKE v2 を使用する必要があります。選択されると、「**DH グループ**」、「**暗号化**」、および「**認証**」フィールドは淡色表示となり、定義できなくなります。

16 「**IKE (フェーズ 1) プロポーザル**」の下の、残りのオプションの数値を設定します。「**DH グループ**」、「**暗号化**」、「**認証**」、および「**存続期間**」の既定値はほとんどの VPN 設定に使用できます。

メモ：「**鍵交換モード**」フィールドにおいて「**IKEv2 モード**」が選択されている場合、「**DH グループ**」、「**暗号化**」、および「**認証**」フィールドは淡色表示となり、これらのオプションに対する選択はできません。

メモ：トンネルの反対側のフェーズ 1 の値が一致するように設定してください。

a 「**メイン モード**」または「**アグレッシブ モード**」の場合、「**DH グループ**」に対して、いくつかの Diffie Hellman 鍵交換から選択できます。

Suite B 暗号に含まれる Diffie Hellman グループ	その他の Diffie-Hellman オプション
256 ビット ランダム ECP グループ	グループ 1
384 ビット ランダム ECP グループ	グループ 2
521 ビット ランダム ECP グループ	グループ 5
192 ビット ランダム ECP グループ	グループ 14
224 ビット ランダム ECP グループ	

b 「**メイン モード**」または「**アグレッシブ モード**」を選択した場合は、「**暗号化**」フィールドでドロップダウン メニューから「**DES**」、「**3DES**」、「**AES-128**」(既定)、「**AES-192**」、または「**AES-256**」を選択します。

c 「**メイン モード**」または「**アグレッシブ モード**」が選択されている場合、「**認証**」フィールドに対して、高度な認証セキュリティのために**MD5**、**SHA-1**(既定)、**SHA256**、**SHA384**、または **SHA512** を選択します。

17 すべての「**鍵交換**」モードについて、「**存続期間 (秒)**」を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

18 「**IPsec (フェーズ 2) プロポーザル**」セクションで、オプションを設定します。「**プロトコル**」、「**暗号化**」、「**認証**」、「**Perfect Forward Secrecy を有効にする**」、および「**存続期間 (秒)**」の既定値は、ほとんどの VPN SA 設定に使用できます。

メモ：トンネルの反対側のフェーズ 2 の値が一致するように設定してください。

a 「**プロトコル**」で、目的のプロトコルを選択します。

「**プロトコル**」フィールドで「**ESP**」を選択した場合は、「**暗号化**」フィールドで、Suite B 暗号化に含まれる以下の 6 つの暗号化アルゴリズムを選択できます。

Suite B 暗号化オプション	その他のオプション
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**なし**

「**プロトコル**」フィールドで「**AH**」を選択した場合、「**暗号化**」フィールドは淡色表示になり、オプションは選択できません。

b 「**認証**」で、使用する認証方式を選択します。選択肢は、「**MD5**」、「**SHA1**」(既定)、「**SHA256**」、「**SHA384**」、「**SHA512**」、「**AES-XCBC**」、または「**なし**」です。

c 追加のセキュリティ層として Diffie-Helman 鍵交換を追加する場合は、「**Perfect Forward Secrecy を有効にする**」を選択します。そして、「**DH グループ**」から「**グループ 2**」を選択します。

d 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

19 「**詳細設定**」を選択します。

IKEv2 モードを使用したサードパーティ証明書の詳細

メイン モードまたはアグレッシブ モードでのサードパーティ証明書の詳細

20 VPN ポリシーに適用する設定オプションを選択します。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
詳細設定		
キープ アライブを有効にする	この VPN トンネルでピア間のハートビート メッセージを使用する場合に選択します。トンネルの一方の側が失敗した場合、キープアライブ ハートビートを使用することにより、両サイドが再び利用可能になったときにトンネルの自動的な再ネゴシエートが可能になります。 提案された存続期間が期限切れになるまで待つ必要はありません。 **メモ**：キープ アライブのオプションは、VPN ポリシーが VPN を越えた DHCP のセントラル ゲートウェイとして設定されている場合、または、プライマリ ゲートウェイ名またはアドレスが 0.0.0.0 である場合は、無効になります。	IKEv2 モードでは選択できません。
この VPN ポリシーに対してアクセス ルールを自動生成しない	*選択しない* (既定) と、付随するアクセス ルールが自動的に作成されます。詳細については、「VPN が自動的に追加するルール コントロール (23 ページ)」を参照してください。	*選択しない* (既定) と、付随するアクセス ルールが自動的に作成されます。詳細については、「VPN が自動的に追加するルール コントロール (23 ページ)」を参照してください。
IPsec アンチリプレイを無効にする	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。
XAUTH を利用した VPN クライアントの認証を要求する	この VPN ポリシーのすべての受信トラフィックは、XAUTH/RADIUS で認証されたユーザからのものである必要があります。認証されていないトラフィックは VPN トンネルでは許可されません。	IKEv2 モードでは使用できません。
Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
マルチキャストを有効にする	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/ 映像アプリケーション) が VPN トンネルを通過できるようにします。	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/ 映像アプリケーション) が VPN トンネルを通過できるようにします。
WXA グループ	**なし** (既定値) または**グループ 1** を選択します。	**なし** (既定値) または**グループ 1** を選択します。
Suite B 互換アルゴリズムのみを表示する	Suite B 互換アルゴリズムのみを表示したい場合に選択します。	Suite B 互換アルゴリズムのみを表示したい場合に選択します。
NAT ポリシーを適用する	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。
OCSP 確認を有効にする	VPN 認証状況を確認したい場合に選択します。フィールドには **OCSP 確認用 URL** を入力します。	VPN 認証状況を確認したい場合に選択します。フィールドには **OCSP 確認用 URL** を入力します。
SonicPointN レイヤ 3 管理を許可する	アクセス ポイントのレイヤ 3 管理を許可します。	アクセス ポイントのレイヤ 3 管理を許可します。
この SA を経由しての管理	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、「**HTTPS**」、「**SSH**」、「**SNMP**」、またはこの 3 つを組み合わせて選択します。	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、「**HTTPS**」、「**SSH**」、「**SNMP**」、またはこの 3 つを組み合わせて選択します。
この SA を経由してのユーザ ログイン	「**HTTP**」、「**HTTPS**」、またはその両方を選択すると、SA を使用したログインがユーザに許可されます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。	「**HTTP**」、「**HTTPS**」、またはその両方を選択すると、SA を使用したログインがユーザに許可されます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
デフォルト LAN ゲートウェイ (オプション)	トンネルに入る前の LAN を通じて未知のサブネットに向けたトラフィックをルーティングしたい場合、このオプションを選択してください。例えば、「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」(「**リモート ネットワーク**」の下の、このページの「**ネットワーク**」表示) が選択されている場合、ルータのアドレスを入力してください。	トンネルに入る前の LAN を通じて未知のサブネットに向けたトラフィックをルーティングしたい場合、このオプションを選択してください。例えば、「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」(「**リモート ネットワーク**」の下の、このページの「**ネットワーク**」表示) が選択されている場合、ルータのアドレスを入力してください。
VPN ポリシーの適用先	ドロップダウン リストからインターフェースかゾーンを選択します。WAN の負荷分散を使用していて、VPN でいずれかの WAN インターフェースを使用する場合は、ゾーン WAN が推奨される選択です。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。	ドロップダウン リストからインターフェースかゾーンを選択します。WAN の負荷分散を使用していて、VPN でいずれかの WAN インターフェースを使用する場合は、ゾーン WAN が推奨される選択です。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。
セカンダリ ゲートウェイを先制する	指定した時間の後に 2 番目のゲートウェイを先制 (プリエンプト) するには、このチェックボックスをオンにし、「**プライマリ ゲートウェイ検知間隔 (秒)**」オプションで目的の時間を設定します。既定の時間は 28800 秒、つまり 8 時間です。	指定した時間の後に 2 番目のゲートウェイを先制 (プリエンプト) するには、このチェックボックスをオンにし、「**プライマリ ゲートウェイ検知間隔 (秒)**」オプションで目的の時間を設定します。既定の時間は 28800 秒、つまり 8 時間です。
IKEv2 設定		
IKE SA ネゴシエーション中に、トリガー パケットを送信しない	メイン モードまたはアグレッシブ モードでは使用できません。	選択されてい「*ない*」 (既定)ピアがトリガー パケットを処理できない場合の相互運用性のために必要な場合のみ、オンにしてください。 セキュリティ ポリシー データベースから適切な保護 IP アドレス範囲を選択できるように IKEv2 応答側を支援するためにトリガー パケットを含めることをお勧めします。すべての実装でこの機能がサポートされているわけではないので、一部の IKE ピアでトリガー パケットを含めないようにしたほうがよいかもしれません。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
ハッシュと URL 証明書種別を受け入れる	メイン モードまたはアグレッシブ モードでは使用できません。	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器に対して HTTP 証明書検索がサポートされているというメッセージを送信します。
ハッシュと URL 証明書種別を送信する	メイン モードまたはアグレッシブ モードでは使用できません。	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器からのメッセージに応答して、HTTP 証明書検索がサポートされているという内容を確認します。

21 「**OK**」を選択します。

22 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

リモート SonicWall ネットワーク セキュリティ装置の設定

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 「**追加**」を選択します。「**VPN ポリシー**」ダイアログが表示されます。

3 「**一般**」画面で、「**認証方式**」ドロップダウン メニューから「**手動鍵 (マニュアル キー)**」を選択します。

4 SA の名前を「**名前**」フィールドに入力します。

5 「**IPSec ゲートウェイ名またはアドレス**」フィールドにローカル接続のホスト名または IP アドレスを入力します。

6 「**ネットワーク**」をクリックします。

7 「**ローカル ネットワーク**」の下で、次のいずれかを選択します。

- 特定のローカル ネットワークが VPN トンネルにアクセス可能である場合は、「**ローカル ネットワークをリストより選択**」ドロップダウン メニューからローカル ネットワークを選択します。
- 任意のローカル ネットワークからトラフィックを発信できる場合は、「**すべてのアドレス**」を選択します。このオプションは、ピアで「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」が選択されている場合に使用します。保護ゾーンと VPN ゾーンの間に、自動追加のルールが作成されます。

8 「**リモート ネットワーク**」の下で、次のいずれかを選択します。

- どのローカル ユーザによるトラフィックも暗号化されていなければファイアウォールから出られないようにするには、「**この VPN トンネルをすべてのインターネット トラフィックのデフォルト ルートとして使用する**」を選択します。

  メモ：この設定を使用する場合は、SA を 1 つだけ設定できます。

- あるいは、「**対象先ネットワークをリストから選択**」を選択して、アドレス オブジェクトまたはグループを選択します。

9 「**プロポーザル**」を選択します。

10 「**受信 SPI**」および「**送信 SPI**」を定義します。SPI は 16 進数 (0123456789abcdef) なので、長さは 3〜8 文字の範囲です。

メモ：各 SA には一意の SPI が必要で、2 つの SA が同じ SPI を共有することはできません。ただし、各 SA の受信 SPI は送信 SPI と同一である可能性があります。

11 「**プロトコル**」、「**暗号化**」、および「**認証**」の既定値は、ほとんどの VPN SA 設定に使用できます。

メモ：「プロトコル」、「暗号化」、および「認証」の値は、トンネルの反対側の値と一致する必要があります。

12 「**暗号化鍵**」フィールドに 48 文字の 16 進数暗号化鍵を入力します。トンネルの反対側のファイアウォールで使用されているのと同じ値を使用します。

13 「**認証鍵**」フィールドに 40 文字の 16 進数認証鍵を入力使用します。トンネルの反対側のファイアウォールで使用されているのと同じ値を使用します。

ヒント：有効な 16 進数の文字とは、0、1、2、3、4、5、6、7、8、9、a、b、c、d、e、および f です。例えば、1234567890abcdef は有効な DES または ARCFour 暗号キーの例です。不適切な暗号キーを入力すると、ブラウザ ウィンドウの下部にエラー メッセージが表示されます。

14 「**詳細設定**」を選択します。

15 GroupVPN ポリシーに適用する次のオプション設定をすべて選択します。

- 「**この VPN ポリシーに対してアクセス ルール自動生成をしない**」設定は既定で有効になっていないので、VPN トラフィックは適切なゾーンを通過できます。
- 「**Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする**」- Windows の「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできます。
- 「**WXA グループ**」で、「**なし**」または「**グループ 1**」を選択します。
- ファイアウォールでローカル、リモート、または両方のネットワーク通信を VPN トンネル経由で変換するには、「**NAT ポリシーを適用する**」を選択します。2 つのドロップダウン メニューが表示されます。
  - ローカル ネットワークでネットワーク アドレス変換を実行するには、「**変換後のローカル ネットワーク**」メニューでアドレス オブジェクトを選択または作成します。
  - リモート ネットワークを変換するには、「**変換後のリモート ネットワーク**」ドロップダウン メニューでアドレス オブジェクトを選択または作成します。

  メモ：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。

- リモート SonicWall を VPN トンネル経由で管理するには、「**この SA を経由しての管理**」から「**HTTP**」、「**SSH**」、「**SNMP**」、またはこの 3 つを任意の組み合わせで選択します。
- 「**この SA を経由してのユーザ ログイン**」で「**HTTP**」または「**HTTPS**」、あるいは両方を選択すると、SA を使用してログインできます。

  メモ：リモート認証を使用した HTTP ユーザ ログインは許可されません。

- ゲートウェイの IP アドレスがある場合は、「**デフォルト LAN ゲートウェイ (オプション)**」フィールドに入力します。
- 「**VPN ポリシーの適用先**」メニューからインターフェースを選択します。

  重要：VPN ゲートウェイの IP アドレスが両方で同じ場合、「**VPN ポリシーの適用先**」ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。

16 「**OK**」を選択します。

17 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

ヒント：Windows ネットワーク (NetBIOS) が有効になっているため、ユーザは Windows の「ネットワーク コンピュータ」でリモート コンピュータを表示することができます。また、サーバまたはワークステーションのリモート IP アドレスを入力することによってリモート LAN のリソースにアクセスすることもできます。

静的ルートへの VPN フェイルオーバーの設定

VPN トンネルが停止した場合に、静的ルートをセカンダリ ルートとして使用できるように設定するためのオプションがあります。「**VPN パスを優先させる**」オプションを使用すると、VPN トンネルのセカンダリ ルートを作成できます。同じ目的アドレス オブジェクトを持つ VPN トラフィックを優先させます。このため、以下のような動作になります。

- VPN トンネルがアクティブな場合:「**VPN パスを優先させる**」オプションが有効であれば、VPN トンネルと送信先アドレス オブジェクトが一致する静的ルートが自動的に無効になります。すべてのトラフィックが VPN トンネルを通って送信先アドレス オブジェクトへ向かいます。
- VPN トンネルが停止した場合、VPN トンネルと送信先アドレス オブジェクトが一致する静的ルートが自動的に有効になります。送信先アドレス オブジェクトへ向かうすべてのトラフィックが静的ルートを通ります。

ネットワーク ルーティング ポリシー設定の詳細は、*SonicOS 6.5 システム設定* を参照してください。

静的ルートを VPN のフェイルオーバーとして設定するには、以下の手順に従います。

1 「**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。

2 「**ルート ポリシー > 追加**」をクリックします。

3 「**名前**」フィールドにポリシーに対するわかりやすい名前を入力します。

4 「**送信元**」、「**送信先**」、「**サービス**」、「**インターフェース**」、および「**ゲートウェイ**」を正しく選択します。

5 **メトリック** は **1** のままにします。

6 「**VPN パスの優先を許可する**」を選択します。

7 「**OK**」を選択します。

3

VPN 自動プロビジョニング

さまざまな種類の IPsec VPN ポリシーが設定可能です。例えば、GroupVPN を含むサイト間 VPN ポリシー、およびルートベース VPN ポリシーなどです。この種のポリシーに対する設定の詳細については、以下のセクションに移動してください。

- サイト間 VPN
- トンネル インターフェースルート ベース VPN

このセクションのトピック:

- VPN 自動プロビジョニング について
- VPN AP サーバの設定
- VPN AP クライアントの設定

VPN 自動プロビジョニング について

SonicOS の VPN 自動プロビジョニング 機能は、2 つの SonicWall ファイアウォールの間でのサイト間 VPN のプロビジョニングを簡素化します。このセクションでは、概念的な情報を提供し、VPN 自動プロビジョニング 機能を設定して使用する方法について説明します。

トピック:

- VPN 自動プロビジョニング の設定
- VPN 自動プロビジョニング の利点
- VPN 自動プロビジョニング の動作

VPN 自動プロビジョニング の設定

VPN 自動プロビジョニング 機能は、SonicWall ファイアウォールの VPN プロビジョニングを簡素化します。これは大規模な VPN 展開で特に便利です。古典的なハブアンドスポーク型の VPN 設定には、セキュリティ関連付けや保護されたネットワークの設定など、スポーク側で必要になる複雑な設定タスクが数多くあります。リモート ゲートウェイが多数ある大規模な配備 (スポーク) では、これが問題になることがあります。VPN 自動プロビジョニング は、リモート VPN ピアでの多くの設定手順が不要になる簡素化された設定プロセスを実現します。

メモ：ハブアンドスポーク型のサイト間 VPN 設定における***ハブ***は、サーバ、ハブ ゲートウェイ、プライマリ ゲートウェイ、セントラル ゲートウェイなど、さまざまな名前で呼ばれることがあります。VPN 自動プロビジョニング 機能のコンテキストでは、***VPN AP サーバ***という用語がハブの代わりに使用されます。同様に、***VPN AP クライアント***という用語は、スポーク クライアント、リモート ゲートウェイ、リモート ファイアウォール、またはピア ファイアウォールに言及するために使用されます。

VPN 自動プロビジョニング の利点

VPN 自動プロビジョニング 機能の明らかな利点は使いやすさにあります。この利点は、SonicWall グローバル VPN クライアント (GVC) のプロビジョニング処理の場合と同様、初期設定の複雑さが SonicOS 管理者に見えないようにすることで実現されます。

SonicWall GVC を使用する際には、ユーザがこの GVC でゲートウェイを指すようにするだけで、セキュリティや接続の設定が自動的に行われます。VPN 自動プロビジョニング は、サイト間のハブアンドスポーク設定のプロビジョニングのために同様のソリューションを提供しており、大規模な配備を簡素化してわずかな手間で済むようにします。

追加の利点として、初期 VPN の自動プロビジョニングの後、ポリシーの変更をセントラル ゲートウェイで制御したり、スポーク エンドで自動的に更新したりできる点が挙げられます。このソリューションは、中央での管理が最優先事項となる、エンタープライズおよび管理サービスの配備で特に魅力的です。

VPN 自動プロビジョニング の動作

VPN 自動プロビジョニング に必要な手順は 2 つあります。

- セントラル ゲートウェイ (VPN AP サーバ) を対象とした SonicWall 自動プロビジョニング サーバの設定
- リモート ファイアウォール (VPN AP クライアント) を対象とした SonicWall 自動プロビジョニング クライアントの設定

どちらの設定も、SonicOS の「**VPN > 基本設定**」ページで VPN ポリシーを追加することによって行います。

サーバ モードでは、セキュリティ関連付け (SA)、保護されたネットワーク、およびその他の設定フィールドを古典的なサイト間 VPN ポリシーと同じように設定します。クライアント モードでは、必要な設定が限られています。ほとんどの場合、リモート ファイアウォール管理者はピア サーバ (セントラル ゲートウェイ) に接続するための IP アドレスを設定するだけで済み、これで VPN を確立できます。

メモ：SonicWall では、1 台の装置に対して AP サーバと AP クライアントの設定を同時に行うことを推奨していません。

VPN 自動プロビジョニング は、クライアント側ではシンプルですが、それでも IP セキュリティの不可欠な要素を提供しています。

アクセス制御
ネットワーク アクセス制御は VPN AP サーバによって実現されます。VPN AP クライアントの観点から見ると、宛先ネットワークは完全に VPN AP サーバ管理者の管理下にあります。ただし、VPN AP クライアントのローカル ネットワークへのアクセスを制御するためのメカニズムが用意されています。

認証
認証は、マシン認証資格情報によって実現されます。IPsec プロポーザルのフェーズ 1 では、インターネット鍵交換 (IKE) プロトコルにより、*事前共有鍵*または *デジタル署名*を用いたマシンレベルの認証が実現されます。VPN ポリシーを設定する際には、以下の認証方式のいずれかを選択できます。

事前共有鍵による認証方式では、管理者が VPN 自動プロビジョニング クライアント ID と鍵 (秘密) を入力します。デジタル署名による認証方式では、管理者がファイアウォールのローカル証明書ストアからクライアント ID を含む X.509 証明書を選択します。この証明書はファイアウォール上に前もって保存しておく必要があります。

	セキュリティ向上のために、XAUTH によるユーザ レベルの資格情報がサポートされています。このユーザ資格情報は、VPN ポリシーの追加時に入力されます。XAUTH では、鍵またはマジック Cookie を使用して、ユーザ資格情報を承認レコードとして抽出します。ユーザがユーザ名とパスワードを動的に入力できるチャレンジ/レスポンスのメカニズムは使用されません。このユーザ資格情報は、追加の認証を実現するだけでなく、VPN AP クライアントによって使用されるリモート リソースやローカル プロキシ アドレスに対するさらなるアクセス制御を実現します。ユーザ資格情報を使用すると、その後のネットワーク プロビジョニングをそれまでとは別のものにすることで、単一の VPN AP サーバ ポリシーを複数の VPN AP クライアント デバイス間で共有できます。
データの機密性と整合性	データの機密性と整合性は、IPsec プロポーザルのフェーズ 2 で、カプセル化セキュリティ ペイロード (ESP) 暗号スイートによって実現されます。

VPN AP クライアント設定に影響するポリシー変更が VPN AP サーバ で行われると、VPN AP サーバは、IKE の re-key (キー更新) メカニズムを使用して、適切なパラメータによる新しいセキュリティ関連付けが確実に確立されるようにします。

IKE フェーズ 1 セキュリティ関連付けの確立について

VPN AP クライアントは使いやすさを目的としているので、多くの IKE および IPsec パラメータは既定値が設定されるか、自動ネゴシエーションが行われます。VPN AP クライアントは、セキュリティ関連付けの確立を開始しますが、開始時には VPN AP サーバの設定を知りません。

IKE フェーズ 1 を確立できるようにするために、使用可能な選択肢のセットは制限されています。VPN AP クライアントは VPN AP サーバがその設定値の選択元として使用できる複数の変換 (セキュリティ パラメータの組み合わせ) を提案します。フェーズ 1 の変換には次のパラメータが含まれます。

- 認証 - 次のいずれかです。
  - PRESHRD - 事前共有鍵を使用します。
  - RSA_SIG - X.509 証明書を使用します。
  - SW_DEFAULT_PSK - 既定のプロビジョニング キーを使用します。
  - XAUTH_INIT_PRESHARED - 事前共有鍵と XAUTH ユーザ資格情報の組み合わせを使用します。
  - XAUTH_INIT_RSA - X.509 証明書と XAUTH ユーザ資格情報の組み合わせを使用します。
  - SW_XAUTH_DEFAULT_PSK - 既定のプロビジョニング キーと XAUTH ユーザ資格情報の組み合わせを使用します。

  上記のすべての変換には、フェーズ 1 プロポーザル設定向けの制限された値または既定値が含まれています。
  - 鍵交換モード - アグレッシブ モード
  - 暗号化 - AES-256
  - ハッシュ - SHA1
  - DH グループ - Diffie Hellman グループ 5
  - 存続期間 (秒) - 28800

VPN AP サーバは、VPN AP クライアント プロポーザルに含まれているものから変換を 1 つ選択することで、応答します。VPN AP サーバが XAUTH 認証方式を使用する変換を選択した場合、VPN AP クライアントはフェーズ 1 完了後に行われる XAUTH チャレンジまで待機します。XAUTH 以外の変換が選択

された場合は、プロビジョニング フェーズが開始されます。VPN AP サーバは、共有鍵 (VPN AP サーバで設定されている場合) や、VPN AP サーバで設定された VPN AP クライアント ID を含む適切なポリシー値を VPN AP クライアントに提供します。

フェーズ 1 SA の確立とポリシー プロビジョニングの完了後、宛先ネットワークが「**VPN > 設定**」ページの「**VPN ポリシー**」セクションに表示されます。

プロビジョニングされたポリシーを使用した IKE フェーズ 2 の確立について

VPN AP プロビジョニング トランザクション中に受け取った値は、その後のフェーズ 2 セキュリティ関連付けを確立するために使用されます。宛先ネットワークごとに別のフェーズ 2 SA が開始されます。フェーズ 2 SA ネゴシエーションをトリガーするために、トラフィックはリモート側の背後から開始する必要があります。この SA は、「**ネットワーク**」画面で VPN AP サーバ ポリシーを設定するときに指定したアドレス オブジェクトに基づいて作成されます (「「ネットワーク」画面での VPN AP サーバの設定 (80 ページ)」を参照)。

メモ：AP サーバ上の同じ VPN ポリシーが複数のリモート AP クライアントで共有されている場合は、それぞれのリモート ネットワークが一意のアドレス オブジェクトとして明確にリストされている必要があります。「**ネットワーク**」画面で VPN AP サーバ ポリシーの設定中に個々のアドレス オブジェクトを「**リモート ネットワーク**」セクションへ追加するとき、アドレス グループに集約できます。単一のアドレス オブジェクトを使用して複数のリモート ネットワークを集約することはできません。SA は*特定の*アドレス オブジェクトに基づいて構築されているためです。

成功した場合、結果として得られたトンネルが「**現在アクティブな VPN トンネル**」に表示されます。

また、NAT ルールが「**ネットワーク > NAT ポリシー**」テーブルに追加されます。

フェーズ 2 パラメータのプロビジョニングは VPN AP サーバによって行われるので、設定の不一致が生じることはありません。VPN AP サーバでフェーズ 2 パラメータが変更された場合は、すべてのフェーズ 1 およびフェーズ 2 セキュリティ関連付けの削除と再ネゴシエーションが実行され、ポリシーの同期が確実に行われます。

VPN AP サーバの設定

VPN AP サーバ設定は、SonicOS の「**VPN > 設定**」ページで VPN ポリシーを追加することによって、サーバ (ハブ) ファイアウォール上で行います。

説明する設定項目の数が多いため、この設定については以下に示す複数のセクションで説明します。

- VPN AP サーバ設定の開始
- 「一般」画面での VPN AP サーバの設定
- 「ネットワーク」画面での VPN AP サーバの設定
- 「プロポーザル」画面での詳細設定
- 「詳細」画面での詳細設定

VPN AP サーバ設定の開始

VPN 自動プロビジョニング を使用して VPN AP サーバ ファイアウォール設定を開始するには、以下の手順に従います。

1 「**VPN > 設定**」ページに移動します。

2 「**表示する IP バージョン**」で「**IPv4**」を選択します。

3 「**VPN ポリシー**」テーブルの下で、「**追加**」を選択します。「**VPN ポリシー**」ダイアログが表示されます。

4 「**認証方式**」ドロップダウン メニューで、「**SonicWall 自動プロビジョニング サーバ**」を選択します。表示が変更されます。

メモ：ページの下部にある**詳細.../非表示**ボタンにより、「**プロポーザル**」タブと「**詳細設定**」タブ オプションの表示が切り替わります。これら 2 つのオプションの設定項目には、管理者の判断によって変更できる既定値が含まれています。

「一般」画面での VPN AP サーバの設定

「一般」画面で VPN AP サーバを設定するには:

1 「**名前**」フィールドに、VPN ポリシーに対するわかりやすい名前を入力します。

2 「**認証方式**」では、次のどちらかを選択します。

- **事前共有鍵** - 次のステップで入力する VPN 自動プロビジョニング クライアント ID と共有鍵を使用します。このオプションは、既定では選択されています。ステップ 3 に進んでください。
- **証明書** - 次のステップで選択する X.509 証明書を使用します (この証明書は前もって装置に保存されている必要があります)。ステップ 9 に進みます。

> **メモ**：VPN AP サーバ ポリシーを (ハブアンドスポーク型の配備と同じように) 共有する必要がある場合、SonicWall では本来の認証を提供して中間者攻撃を防ぐために X.509 証明書を使用することを推奨します。

3 「**認証方式**」で「**事前共有鍵**」を選択した場合は、「**SonicWall 設定**」の下にある「**VPN AP クライアント ID**」フィールドに VPN 自動プロビジョニング クライアント ID を入力します。このフィールドは「**名前**」フィールドに入力した値に応じて自動的に作成されますが、変更可能です。

> **メモ**：この VPN ポリシー値は AP サーバ側と AP クライアント側の双方で一致している必要があります。また、単一の AP サーバ ポリシーを使用して複数の AP クライアントを終了することもできます。

4 VPN AP クライアントがすべての SonicWall 装置に知られている既定の鍵を*最初の*セキュリティ関連付けに使用できるようにするには、「**既定のプロビジョニング鍵を使用する**」チェックボックスを選択します。この SA が確立されると、VPN AP サーバで設定されている**事前共有鍵**が今後の使用のために VPN AP クライアントに提供されます。

このチェックボックスが選択されていない場合、VPN AP クライアントは設定されている共有鍵を使用する必要があります。これにより、管理者は VPN AP サーバでのみ設定されている共有鍵を変更したうえで、新しい共有鍵の値を用いて VPN AP クライアントを更新するために既定のプロビジョニング鍵の使用を簡単に許可することができます。

> **メモ**：最高のセキュリティを得るために、SonicWall では、VPN AP クライアントに共有鍵を提供できるとともに管理者による吟味が行われる短い期間についてのみ、「既定のプロビジョニング鍵」オプションを有効にすることを推奨します。

5 必要に応じて、「**事前共有鍵**」フィールドに何らかの入力を行う前に、「**事前共有鍵を隠す**」チェックボックスの選択を解除します。このチェックボックスは既定で選択されており、その場合は入力した文字が非表示になります。このチェックボックスを再び選択すると、「**事前共有鍵**」フィールドの値が「**事前共有鍵の確認**」フィールドに自動的にコピーされます。

6 「**事前共有鍵**」フィールドに共有鍵を入力します。少なくとも 4 文字を入力する必要があります。

「**既定のプロビジョニング鍵を使用する**」チェックボックスが選択されている場合、VPN AP サーバで設定されている「**事前共有鍵**」がプロビジョニング時に VPN AP クライアントに提供されます。「**既定のプロビジョニング鍵を使用する**」チェックボックスの選択が解除されている場合は、この共有鍵が VPN AP クライアントでも設定されている必要があります。

7 「**事前共有鍵の確認**」フィールドに共有鍵をもう一度入力します。この値は「**事前共有鍵**」フィールドに入力したものと一致している必要があります。

8 「ステップ 12」に移動します。

9 「**認証方式**」で「**証明書**」を選択した場合は、「**SonicWall 設定**」の下にある「**ローカル証明書**」ドロップダウン メニューから適切な証明書を選択します。

10 「**VPN AP クライアント ID 種別**」ドロップダウン メニューから次のいずれかを選択します。

- **識別名 (DN)**
- **電子メール ID (ユーザ FQDN)**
- **ドメイン名 (FQDN)**
- **IP アドレス (IPv4)**

11 「**VPN AP クライアント フィルタ**」には、クライアントを検証するための IKE ネゴシエーション時に提示される証明書 ID に適用する一致文字列またはフィルタを入力します。

12 続きは「「ネットワーク」画面での VPN AP サーバの設定」で説明します。

「ネットワーク」画面での VPN AP サーバの設定

「ネットワーク」画面で VPN AP サーバを設定するには:

1 「**ネットワーク**」をクリックします。

2 「**ローカル ネットワーク**」の下で、「**XAUTH を介した VPN AP クライアントの認証を要求する。**」チェックボックスを選択して、SA の確立時にセキュリティ向上のためにユーザ資格情報の使用を強制します。

3 XAUTH オプションが有効になっている場合は、「**XAUTH に使用するユーザ グループ**」ドロップダウン メニューから許可するユーザのユーザ グループを選択します。「*Trusted Users*」のような既存のグループまたは別の標準グループを選択することも、カスタム グループを作成するために「**ユーザ グループの作成**」を選択することもできます。

認証される各ユーザについて、認証サービスはプロビジョニング交換時に VPN AP クライアントに送信される 1 つ以上のネットワーク アドレスを返します。

XAUTH が有効になっていてユーザ グループが選択されている場合、VPN AP クライアント側のユーザは、認証を成功させるために次の条件を満たしている必要があります。

- ユーザは選択したユーザ グループに属している必要がある。
- ユーザは「**管理 | システム セットアップ | ユーザ > 設定 > ユーザ認証方式**」で設定されているユーザ認証方式をパスできる。
- ユーザは VPN アクセス権限を持っている。

4 XAUTH オプションが無効になっている場合は、ネットワーク アドレス オブジェクトまたはグループを「**認証されていない VPN AP クライアントのアクセス許可**」ドロップダウン メニューから選択するか、「**アドレス オブジェクト/グループの新規作成**」を選択してカスタム オブジェクトまたはグループを作成します。選択したオブジェクトは、この VPN 接続経由でアクセスできるアドレスおよびドメインのリストを定義しています。このオブジェクトは、プロビジョニン

グ交換時に VPN AP クライアントに送信され、その後 VPN AP クライアントのリモート プロキシ ID として使用されます。

5 「**リモート ネットワーク**」で、次のいずれかのラジオ ボタンを選択し、該当する場合は、関連付けられているリストからの選択を行います。

- **対象先ネットワークをリストから選択してください。** - VPN AP クライアント側のルーティング可能な実際のネットワークであるリモート アドレス オブジェクトのドロップダウン メニューからネットワーク オブジェクトを選択するか、カスタム オブジェクトを作成します。

  メモ：VPN 自動プロビジョニング は、AP クライアントの保護されたすべてのサブネットを含む "スーパー ネットワーク" の使用をサポートしていません。保護されたサブネットの異なる複数の AP クライアントが同じ AP サーバに接続できるようにするには、AP クライアントの保護されたサブネットをすべて含むアドレス グループを設定し、そのアドレス グループを「**対象先ネットワークをリストから選択**」フィールドで使用します。このアドレス グループは、新しい AP クライアントの追加にともない、最新の状態を維持する必要があります。

- **認証サービスを介して NAT プロキシを取得する** - RADIUS サーバがユーザの Framed-IP アドレス属性を返すようにするには、このオプションを選択します。この属性は、トラフィックを IPsec トンネルに送信する前に内部アドレスを NAT によって変換するために VPN AP クライアントによって使用されます。
- **NAT プールの選択** - ドロップダウン メニューからネットワーク オブジェクトを選択するか、カスタム オブジェクトを作成します。選択したオブジェクトは、NAT で使用するために VPN AP クライアントに割り当てるアドレスのプールを指定しています。クライアントは、その内部アドレスを NAT プール内のアドレスに変換してから IPsec トンネルにトラフィックを送信します。

  メモ：VPN 自動プロビジョニング を配備する際には、既存および予期される VPN AP クライアントのすべてに対して十分大きな NAT IP アドレス プールを割り当てる必要があります。そうしないと、プール内のすべての IP アドレスが割り当て済みになった場合に VPN AP クライアントが適切に機能できなくなります。

  メモ：大きな IP プールを設定しても、小さなプールより多くのメモリが消費されるわけではないので、安全のために余るくらいに大きなプールを割り当てます。これがベスト プラクティスです。

6 続きは「「プロポーザル」画面での詳細設定」で説明します。

「プロポーザル」画面での詳細設定

設定されたパラメータは、フェーズ 2 の確立の前に VPN AP クライアントに自動的に提供されます。そのため、VPN AP サーバと VPN AP クライアントとの間に設定の依存関係が生じることはありません。

「プロポーザル」画面で VPN AP サーバを設定するには:

1 「**一般**」または「**ネットワーク**」画面で、「**詳細設定**」ボタンを選択して、「**プロポーザル**」を表示します。

2 「**プロポーザル**」を選択します。

3 「**IKE (フェーズ 1) プロポーザル**」で、フェーズ 1 プロポーザルの存続期間を秒単位で入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

自動プロビジョニングを簡素化するために、このセクションのその他のフィールドは淡色表示になっており、次のように事前設定されています。

- **鍵交換モード: アグレッシブ モード**
- **DH グループ: グループ 5**
- **暗号化: AES-256**
- **認証: SHA1**

4 「**Ipsec (フェーズ 2) プロポーザル**」で、「**暗号化**」ドロップダウン メニューから適切な暗号化アルゴリズムを選択します。既定値は「**AES-128**」です。

「**プロトコル**」フィールドは、淡色表示になっており、カプセル化セキュリティ ペイロード (ESP) 暗号スイートを使用するための「**ESP**」が事前設定されています。

5 「**認証**」ドロップダウン メニューから、適切な認証暗号方式を選択します。既定値は **SHA1** です。

6 セキュリティをさらに強化するために Diffie-Helman 鍵交換を追加する場合は、「**Perfect Forward Secrecy を有効にする**」チェックボックスを選択します。選択した場合、「**DH グループ**」ドロップダウン リストが表示されます。リストから適切なグループを選択します。既定値はグループ 2 です。

7 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

8 続きは「「詳細」画面での詳細設定」で説明します。

「詳細」画面での詳細設定

「詳細」画面で VPN AP サーバを設定するには:

1 「**詳細設定**」を選択します。

2 重複したシーケンス番号を持つパケットが破棄されないようにするには、「**IPsec アンチリプレイを無効にする**」チェックボックスを選択します。

3 ストリーミング オーディオ (VoIP を含みます) やビデオ アプリケーションなどの IP マルチキャスト トラフィックを VPN AP サーバから、このポリシーを使用して確立された任意の VPN AP クライアント SA 経由で流せるようにするには、「**マルチキャストを有効にする**」チェックボックスを選択します。

4 SonicWall WAN 高速化を使用する場合は、「**WXA グループ**」ドロップダウン リストから値を選択します。

5 必要に応じて、「**Suite B 互換アルゴリズムのみを表示する**」を選択します。

6 SonicWall SonicPoint 無線アクセス デバイスを VPN トンネル経由で管理できるようにするには、「**SonicPointN レイヤ 3 管理を許可する**」を選択します。

7 「**この SA を経由しての管理**」では、**HTTPS**、**SSH**、または **SNMP** を使用した VPN トンネル経由の VPN AP サーバの管理をリモート ユーザに許可するためのチェックボックスを 1 つ以上選択します。

8 「**この SA を経由してのユーザ ログイン**」では、**HTTP** または **HTTPS** を使用した VPN トンネル経由のログインをリモート ユーザに許可するためのチェックボックスを 1 つ以上選択します。

9 必要に応じて、「**デフォルト LAN ゲートウェイ (オプション)**」フィールドに VPN AP サーバのデフォルト LAN ゲートウェイの IP アドレスを入力します。ある種のトラフィックで静的ルートが見つからない場合、VPN AP サーバはそのトラフィックを設定されているデフォルト LAN ゲートウェイに転送します。

メモ：このオプションは、一部のバージョンの SonicOS で機能しない可能性があります。

10 この VPN ポリシーを特定のインターフェースまたはゾーンにバインドするには、「**VPN ポリシーの適用先**」ドロップダウン メニューでインターフェースまたはゾーンを選択します。既定値は「**ゾーン WAN**」です。

11 終了したら、「**OK**」をクリックします。

VPN AP クライアントの設定

VPN AP クライアント設定は、SonicOS の「**VPN > 設定**」ページで VPN ポリシーを追加することによって、クライアント ファイアウォール上で行います。

VPN 自動プロビジョニング を使用してリモート クライアント ファイアウォール設定を実行するには、以下の手順に従います。

1 「**VPN > 設定**」ページに移動します。

2 「**表示する IP バージョン**」で「**IPv4**」を選択します。

3 「**VPN ポリシー**」テーブルの下で、「**追加**」を選択します。「**セキュリティ ポリシー**」ダイアログが表示されます。

4 「**認証方式**」ドロップダウン メニューで、「**SonicWall 自動プロビジョニング クライアント**」を選択します。ページの内容が更新され、各種フィールドが表示されます。

5 「**名前**」フィールドに、VPN ポリシーに対するわかりやすい名前を入力します。

6 「**プライマリ IPSec ゲートウェイ名またはアドレス**」フィールドに、完全修飾ドメイン名 (FQDN)、または VPN AP サーバの IPv4 アドレスを入力します。

7 「**認証方式**」では、次のどちらかを選択します。

- **事前共有鍵** - 次のステップで入力する VPN 自動プロビジョニング クライアント ID と共有鍵を使用します。このオプションは、既定では選択されています。ステップ 8 に進んでください。
- **証明書** - 次のステップで選択する X.509 証明書を使用します (この証明書は前もって装置に保存されている必要があります)。ステップ 14 に進みます。

8 「**認証方式**」で「**事前共有鍵**」を選択した場合は、「**SonicWall 設定**」の下にある「**VPN AP クライアント ID**」フィールドに VPN 自動プロビジョニング クライアント ID を入力します。

このクライアント ID は、VPN AP サーバ (**SonicWall 自動プロビジョニング サーバ**として設定されている SonicWall ファイアウォール) の設定によって決定されます。

メモ：この VPN ポリシー値は AP サーバ側と AP クライアント側の双方で一致している必要があります。また、単一の AP サーバ ポリシーを使用して複数の AP クライアントを終了することもできます。

9 必要に応じて、「**既定のプロビジョニング鍵を使用する**」チェックボックスを選択して、すべての SonicWall 装置に知られている既定の鍵を*最初の*セキュリティ関連付けに使用します。この SA が確立されると、VPN AP サーバで設定されている**事前共有鍵**が今後の使用のために VPN AP クライアントに提供されます。

メモ：VPN AP サーバは、既定のプロビジョニング鍵を受け入れるように設定されている必要があります。そうでない場合、SA の確立は失敗します。

「**既定のプロビジョニング鍵を使用する**」を選択した場合は、ステップ 13 に進みます。

10 「**既定のプロビジョニング鍵を使用する**」チェックボックスを選択しなかった場合は、必要に応じて、「**事前共有鍵**」フィールドに何らかの入力を行う前に、「**事前共有鍵を隠す**」チェックボックスの選択を解除します。このチェックボックスは既定で選択されており、その場合は入力した文字が非表示になります。このチェックボックスを再び選択すると、「**事前共有鍵**」フィールドの値が「**事前共有鍵の確認**」フィールドに自動的にコピーされます。

11 「**事前共有鍵**」フィールドに共有鍵を入力します。これは VPN AP サーバで設定されている共有鍵と同じもので、かつ 4 文字以上でなければなりません。

12 「**事前共有鍵の確認**」フィールドに共有鍵をもう一度入力します。この値は「**事前共有鍵**」フィールドに入力したものと一致している必要があります。

13 「**ユーザ設定**」でのユーザ資格情報の入力については、ステップ 15 を参照してください。ユーザ資格情報はオプションです。

14 「**認証方式**」で「**証明書**」を選択した場合は、「**SonicWall 設定**」の下にある「**ローカル証明書**」ドロップダウン メニューから適切な証明書を選択します。

15 「**ユーザ設定**」で、オプションのユーザ資格情報で使用するユーザ名を「**ユーザ名**」フィールドに入力します。このユーザ名はユーザレベルの認証のために XAUTH 経由で送信されます。

16 必要に応じて、「**ユーザ パスワード**」フィールドに何らかの入力を行う前に、「**ユーザ パスワードを隠す**」チェックボックスの選択を解除します。このチェックボックスは既定でオンになっています。オンになっている場合、入力した文字はドットとして表示されます。このチェックボックスの選択を解除すると、値が平文 (プレーン テキスト) で表示され、「**ユーザ パスワード**」フィールドに入力した値が「**ユーザ パスワードの確認**」フィールドに自動的にコピーされます。

17 「**ユーザ パスワード**」フィールドにユーザ パスワードを入力します。

18 「**ユーザ パスワードの確認**」フィールドにもう一度ユーザ パスワードを入力します。

19 準備ができたら、「**OK**」を選択して、VPN ポリシーを追加します。

4

トンネル インターフェースルート ベース VPN

このセクションでは、ルート ベースの VPN ソリューションを提供するトンネル インターフェース VPN ポリシーの設定方法を説明します。トンネル インターフェース VPN ポリシーは、サイト間 VPN ポリシーとは異なり、VPN ポリシーの設定にネットワーク トポロジの設定が必ず含まれるようにします。そのため、トポロジが頻繁に変更されるネットワークでは、VPN ポリシーの設定や保守が難しくなります。詳細については、「サイト間 VPN (25 ページ)」を参照してください。

ルート ベース VPN のアプローチならば、VPN ポリシーの設定時にネットワーク トポロジを設定する必要はありません。VPN ポリシーを設定すると、2 つのエンドポイント間に***番号付けされないトンネル インターフェース***が作成されます。静的または動的ルートをこのトンネル インターフェースに追加することができます。ルート ベース VPN アプローチを使用すれば、ネットワークの設定が VPN ポリシーの設定から静的または動的ルートの設定に移されます。

ルート ベース VPN では、VPN ポリシーの設定や保守が容易になり、トラフィックを柔軟にルーティングできます。そのため、単一または多重 VPN 上で重複するネットワークに対して複数のパスを定義できるようになります。

VPN ネットワークの自動プロビジョニングの詳細については、「VPN 自動プロビジョニング」を参照してください。

トピック:

用語

このセクションでは、以下の用語が使用されます。

VPN トンネル ポリシー	ローカル/リモートの保護ネットワークが存在しないものとして設定されたポリシー。パケット送信時、SonicOS がトンネル ポリシーを検索する必要はありません。
VPN トンネル インターフェース	「**ネットワーク > インターフェース**」ページで作成され、トンネル ポリシーに関連付けられた、番号付けされたトンネル インターフェース。このインターフェースは、ルート登録の送信インターフェースとして、または Net Monitor ポリシーや Syslog ポリシーなどのパケットを能動的に送信する SonicOS 機能の送信インターフェースとして設定されます。論理的に見たとき、SonicOS がパケットを VPN トンネル経由で送信するのは、パケットが暗号化される点を除けば、物理インターフェース経由で送信するのと同じことです。
番号付けされたトンネル インターフェース	番号付けされたトンネル インターフェースは IP アドレスを持ちます。番号付けされたトンネル インターフェースは、「**ネットワーク > インターフェース**」ページで VPN トンネル インターフェースを追加すると作成されます。機能的に、番号付けされたトンネル インターフェースは番号付けされないトンネル インターフェースの上位集合と位置づけられます。番号付けされたトンネル インターフェースは、標準インターフェースと同じように設定できます。HTTPS、Ping、SNMP、SSH 管理用の設定、HTTP および HTTPS のユーザ ログイン、断片化の処理などに対応しています。番号付けされたトンネル インターフェースは、NAT ポリシー、ファイアウォール アクセス制御リスト、すべての種別の動的ルーティング (RIP、OSPF、BGP) を含むルーティング ポリシーを設定する操作に使用できます。
番号付けされていないトンネル インターフェース	番号付けされていないトンネル インターフェースには IP アドレスがありません。番号付けされないトンネル インターフェースは、**トンネル インターフェース**を**ポリシー種別**として VPN ポリシーを設定すると作成されます。既定で、このインターフェースは、単純なルートベースの VPN に使用され、動作するのに IP アドレスを必要としません。ポリシー設定ダイアログの「詳細」画面で「**高度なルーティングを許可する**」オプションを有効にすると、番号付けされないトンネル インターフェースを RIP または OSPF の動的ルーティングに使用できます。番号付けされないトンネル インターフェースを使って RIP または OSPF を設定すると、IP アドレスが物理または論理 (VLAN) インターフェースから借用されます。

トンネル インターフェースの追加

ルート ベース VPN の設定は、次の 2 ステップで行われます。

1 トンネル インターフェースを作成します。2 つのエンドポイント間のトラフィックを保護するための暗号スイートが、このトンネル インターフェース内に定義されます。

2 トンネル インターフェースを用いて静的または動的ルートを作成します。

トンネル インターフェースは、"**トンネル インターフェース**" という種類のポリシーをリモート ゲートウェイに追加すると作成されます。トンネル インターフェースは物理インターフェースにバインドされる必要があり、その物理インターフェースの IP アドレスがトンネルを通るパケットの送信元アドレスとして使用されます。

トンネル インターフェースを追加するには:

1 「**管理 | 接続性 | VPN > 基本設定**」に移動します。

2 「**表示する IP バージョン**」オプションで、「**IPv4**」または「**IPv6**」を選択します。

3 「**追加**」ボタンを選択します。

4 「**一般**」画面で、「**ポリシー種別**」として「**トンネル インターフェース**」を選択します。

5 「**認証方式**」で、次のいずれかを選択します。

- **手動鍵**
- **IKE (事前共有鍵を使用)** (既定)
- **IKE (サード パーティ証明書を使用)**
- **SonicWall 自動プロビジョニング クライアント**
- **SonicWall 自動プロビジョニング サーバ**

「**一般**」画面の残りのフィールドは、選択したオプションに応じて変化します。

使用可能な選択の詳細については、以下を参照してください。

- マニュアル キーを使用する設定 (55 ページ)
- 事前共有鍵を使用する設定 (46 ページ)
- サードパーティ証明書を使った設定 (59 ページ)
- VPN AP クライアントの設定 (84 ページ)
- VPN AP サーバの設定 (77 ページ)

6 「**プロポーザル**」を選択します。

7 「**IKE (フェーズ 1) プロポーザル**」で、「**鍵交換モード**」ドロップダウン メニューから以下のオプションのうち 1 つを選択します。

メイン モード	IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
アグレッシブ モード	通常は WAN アドレッシングが動的に割り当てられる場合に使用されます。IKEv1 フェーズ 1 プロポーザルを IPsec フェーズ 2 プロポーザルとともに使用します。Suite B 暗号化オプションは、IKE フェーズ 1 設定の「DH グループ」と IPsec フェーズ 2 設定の「暗号化」で使用できます。
IKEv2 モード	すべてのネゴシエーションを、IKEv1 のフレーズよりも IKEv2 プロトコルで実行するようにします。 **メモ：IKE v2 モード**を選択する場合は、VPN トンネルの両端で IKE v2 を使用する必要があります。選択されると、「**DH グループ**」、「**暗号化**」、および「**認証**」フィールドは無効になり、定義できなくなります。

8 「**IKE (フェーズ 1) プロポーザル**」の下の、残りのオプションの数値を設定します。「**DH グループ**」、「**暗号化**」、「**認証**」、および「**存続期間 (秒)**」の既定値はほとんどの VPN 設定に使用できます。

メモ：トンネルの反対側のフェーズ 1 の値が一致するように設定してください。

a 「**メイン モード**」または「**アグレッシブ モード**」の場合、「**DH グループ**」に対して、いくつかの Diffie Hellman 鍵交換から選択できます。

Suite B 暗号に含まれる Diffie Hellman グループ	その他の Diffie-Hellman オプション
256 ビット ランダム ECP グループ	グループ 1
384 ビット ランダム ECP グループ	グループ 2
521 ビット ランダム ECP グループ	グループ 5
192 ビット ランダム ECP グループ	グループ 14
224 ビット ランダム ECP グループ	

b 「**メイン モード**」または「**アグレッシブ モード**」を選択した場合は、「**暗号化**」フィールドでドロップダウン メニューから「**DES**」、「**3DES**」、「**AES-128**」(既定)、「**AES-192**」、または「**AES-256**」を選択します。

c 「**メイン モード**」または「**アグレッシブ モード**」が選択されている場合、「**認証**」フィールドに対して、強化された認証セキュリティのために、「**SHA-1**」(既定)、「**MD5**」、「**SHA256**」、「**SHA384**」、または「**SHA512**」から選択してください。

d すべての「**鍵交換**」モードについて、「**存続期間 (秒)**」を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

9 「**Ipsec (フェーズ 2) プロポーザル**」セクションで、オプションを設定します。「**プロトコル**」、「**暗号化**」、「**認証**」、「**Perfect Forward Secrecy を有効にする**」、および「**存続期間 (秒)**」の既定値は、ほとんどの VPN SA 設定に使用できます。

メモ：トンネルの反対側のフェーズ 2 の値が一致するように設定してください。

a 「**プロトコル**」フィールドで、「**ESP**」または「**AH**」を選択します。

b 「**プロトコル**」フィールドで「**ESP**」を選択した場合は、「**暗号化**」フィールドで、Suite B 暗号化に含まれる以下の 6 つの暗号化アルゴリズムを選択できます。

Suite B 暗号化オプション	その他のオプション
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**なし**

メモ：「**プロトコル**」フィールドで「**AH**」を選択した場合、「**暗号化**」フィールドは無効になり、オプションは選択できません。

c **認証**フィールドは、ドロップダウン リストから認証方法を選択します。

- **MD5**
- **SHA1** (既定)
- **SHA256**
- **SHA384**
- **SHA512**

- **AES-XCBC**

d セキュリティ強化を行う場合、「**Perfect Forward Secrecy を有効にする**」を選択します。

e 「**存続期間 (秒)**」フィールドに値を入力します。既定の「**28800**」により、トンネルは 8 時間ごとに鍵の再ネゴシエートと交換を行います。

10 「**詳細設定**」を選択します。

11 以下の詳細オプションを設定できます (既定では、いずれもオフになっています)。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
詳細設定		
キープ アライブを有効にする	ルート ベース インターフェースでは、選択できません。	ルート ベース インターフェースでは、選択できません。
IPsec アンチリプレイを無効にする	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。	IPsec アンチリプレイは、部分的なシーケンス整合性を確保するための機能の 1 つで、(制約されたウィンドウ内の) 重複する IP データグラムの到着を検出します。
高度なルーティングを許可する	このトンネル インターフェースを、「**ネットワーク > ルーティング**」ページの「**ルーティング プロトコル**」テーブル内のインターフェース リストに追加します。	このトンネル インターフェースを、「**ネットワーク > ルーティング**」ページの「**ルーティング プロトコル**」テーブル内のインターフェース リストに追加します。
	メモ：このオプションは、トンネル インターフェースを高度なルーティング (RIP、OSPF) に使う場合に選択する必要があります。これをオプション設定にすることで、「**ルーティング プロトコル**」テーブルにすべてのトンネル インターフェースを追加する必要はなくなり、ルーティング設定が簡易化されます。	
トランスポート モードを有効にする	このオプションは、GRE (汎用ルーティング カプセル化) などの別のトンネリング プロトコルによって既にカプセル化されているパケットを保護するために使用されます。ペイロードと ESP トレーラのみを暗号化するため、元のパケットの IP ヘッダーは暗号化されません。	「**IKEv2 モード**」では使用できません。
Windows ネットワーキング (NetBIOS) ブロードキャストを有効にする	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。	ウィンドウズの「ネットワーク コンピュータ」を参照してリモート ネットワーク リソースにアクセスできるようにします。
マルチキャストを有効にする	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/映像アプリケーション) が VPN トンネルを通過できるようにします。	選択すると、IP マルチキャスト トラフィック (音声 (VoIP など)/映像アプリケーション) が VPN トンネルを通過できるようにします。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
WXA グループ	なし (既定値) またはグループ 1 を選択します。	なし (既定値) またはグループ 1 を選択します。
Suite B 互換アルゴリズムのみを表示する	Suite B 互換アルゴリズムのみを表示したい場合に選択します。	Suite B 互換アルゴリズムのみを表示したい場合に選択します。
NAT ポリシーを適用する	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。	ファイアウォールでローカル ネットワーク、リモート ネットワーク、または両方のネットワーク通信を VPN トンネル経由で変換したい場合に選択します。選択した場合、「**変換されたローカル ネットワーク**」または「**変換されたリモート ネットワーク**」を選択するか、あるいは 2 つのドロップダウン メニューから 1 つずつを選択してください。 **メモ**：通常は、トンネルで NAT が必要な場合、ローカルとリモートの両方ではなくいずれかを変換する必要があります。「**NAT ポリシーを適用する**」は、トンネルの両サイドで同一または重複するサブネットを使用する場合に特に有用です。
SonicPointN レイヤ 3 管理を許可する	SonicPoint N および SonicWave にレイヤ 3 管理を許可します。	SonicPoint N および SonicWave にレイヤ 3 管理を許可します。
この SA を経由しての管理	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、このオプションで「**HTTPS**」、「**SSH**」、「**SNMP**」のいずれかを選択します。	ローカル SonicWall ファイアウォールを VPN トンネル経由で管理するには、このオプションで「**HTTPS**」、「**SSH**」、「**SNMP**」のいずれかを選択します。
この SA を経由してのユーザ ログイン	「**HTTP**」または「**HTTPS**」、あるいは両方を選択すると、SA を使用してログインできます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。	「**HTTP**」または「**HTTPS**」、あるいは両方を選択すると、SA を使用してログインできます。 **メモ**：リモート認証を使用した HTTP ユーザ ログインは許可されません。
VPN ポリシーの適用先	ドロップダウン リストからインターフェースを選択します。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。	ドロップダウン リストからインターフェースを選択します。 **重要**：VPN ゲートウェイの IP アドレスが両方で同じ場合、VPN ポリシーの適用先 ドロップダウン メニューから 2 つの異なる WAN インターフェースを選択することはできません。

オプション	メイン モードまたはアグレッシブ モード	IKEv2 モード
IKEv2 設定		
IKE SA ネゴシエーション中に、トリガー パケットを送信しない	使用不可	選択されてい「*ない*」 (既定)ピアがトリガー パケットを処理できない場合の相互運用性のために必要なときだけ、オンにしてください。 セキュリティ ポリシー データベースから適切な保護 IP アドレス範囲を選択できるように IKEv2 応答側を支援するためにトリガー パケットを含めることをお勧めします。すべての実装でこの機能がサポートされているわけではないので、一部の IKE ピアでトリガー パケットを含めないようにしたほうがよいかもしれません。
ハッシュと URL 証明書種別を受け入れる	使用不可	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器に対して HTTP 証明書検索がサポートされているというメッセージを送信します。
ハッシュと URL 証明書種別を送信する	使用不可	お使いの機器が証明書自体ではなくハッシュと証明書の URL を送信して処理できる場合は、このオプションを選択します。選択されると、相手の機器からのメッセージに応答して、 HTTP 証明書検索がサポートされているという内容を確認します。

12 「**OK**」を選択します。

13 「**VPN > 基本設定**」ページで、「**承諾**」を選択して、VPN ポリシーを更新します。

トンネル インターフェースに対して静的ルートを作成

トンネル インターフェースの追加に成功したら、それに伴う静的ルートを作成します。

トンネル インターフェースへの静的ルートを作成するには:

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

2 「**追加**」ボタンを選択して、「**ルート ポリシーの追加**」ダイアログを表示します。

3 「**インターフェース**」ドロップダウン メニューに表示されている利用可能なすべてのトンネル インターフェースから、トンネル インターフェースを 1 つ選択します。

> **メモ：「自動追加アクセス ルール**」オプションが選択されている場合は、ファイアウォール ルールが自動的に追加され、トンネル インターフェースを使用して設定されたネットワーク間でトラフィックが許可されます。

4 必要に応じて残りの項目を設定します。詳細については、*SonicOS 6.5 システム設定* の「ネットワーク ルーティング」セクションを参照してください。

5 「**OK**」を選択します。

異なるネットワーク セグメントを使用するルート エントリ

トンネル インターフェースを作成した後、異なるネットワークで同じトンネル インターフェースを使用するための、複数のルート エントリを設定することができます。これにより、トンネル インターフェースを何も変更することなくネットワーク トポロジを変更するための仕組みができあがります。

ネットワークへの静的ルートの冗長化

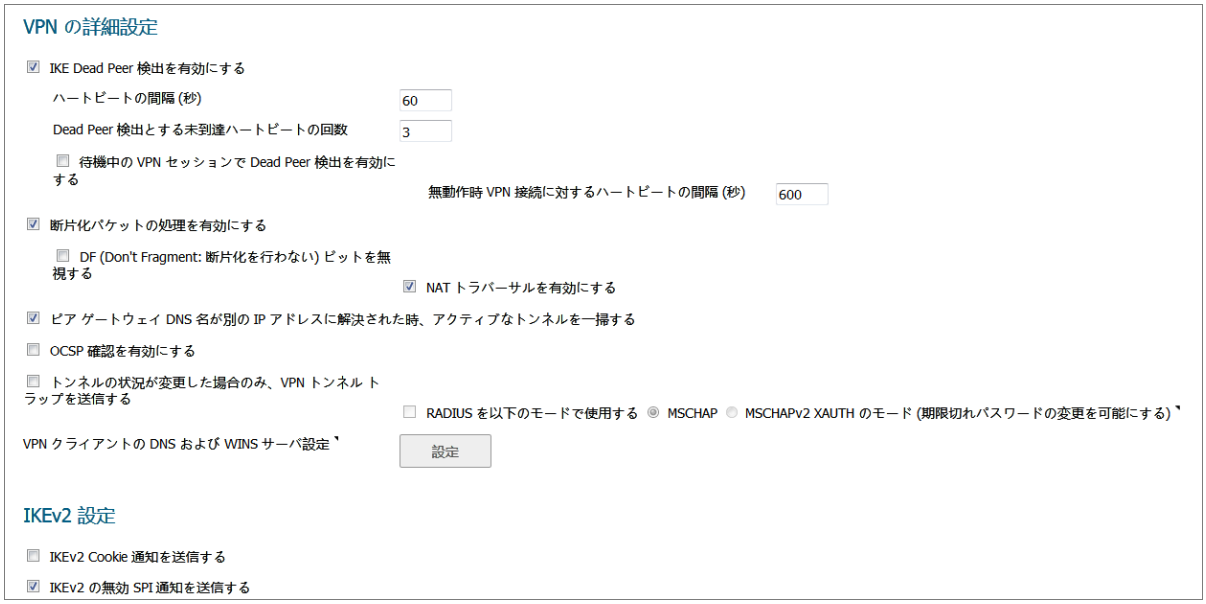
トンネル インターフェースを 2 つ以上設定したら、重複する複数の静的ルートを追加してください。各静的ルートが異なるトンネル インターフェースを使用してトラフィックをルーティングするようにします。こうすることで、送信先に到達するトラフィックのルーティングが冗長化されます。冗長なルートがなければ、静的ルートをドロップ トンネル インターフェースに追加して、VPN トラフィックが既定ルート以外に転送されるのを回避することができます。詳細については、*SonicOS 6.5 システム設定* の「ネットワーク インターフェース」セクションを参照してください。

5

VPN の詳細設定

「**VPN > 詳細**」ページには次の 2 つのセクションがあります。

- **VPN の詳細設定**
- **IKEv2 設定**



トピック:

- VPN の詳細設定
- IKEv2 の設定

VPN の詳細設定

「**VPN の詳細設定**」は、すべての VPN ポリシーに影響を与えます。また、このセクションでは、OCSP (Online Certificate Status Protocol) 用のソリューションについても説明します。OCSP により、CRL (証明書失効リスト) なしで VPN 証明書状況を確認できます。これで、ファイアウォールで使用される証明書の状況に関するアップデートを適時に行うことができます。この章は、次のセクションで構成されています。

- **IKE Dead Peer 検出を有効にする** - アクティブでない VPN トンネルをファイアウォールによって破棄する場合に選択します。
  - **ハートビートの間隔 (秒)** - "ハートビート" 間隔の秒数を入力します。既定値は 60 秒です。

- **Dead Peer 検出とする未到達ハートビートの回数** - 未到達ハートビート回数を入力します。既定値は 3 です。トリガー レベルに達した場合、VPN 接続はファイアウォールにより破棄されます。ファイアウォールは、フェーズ 1 暗号化手順によって保護された UDP パケットを使用します。
- **待機中の VPN セッションで Dead Peer 検出を有効にする** - 「**無動作時 VPN 接続に対するハートビートの間隔 (秒)**」フィールドで定義した時刻の値に到達後、動作していない VPN 接続をファイアウォールによって破棄する場合は、この設定を選択します。既定値は“600" 秒 (10 分) です。

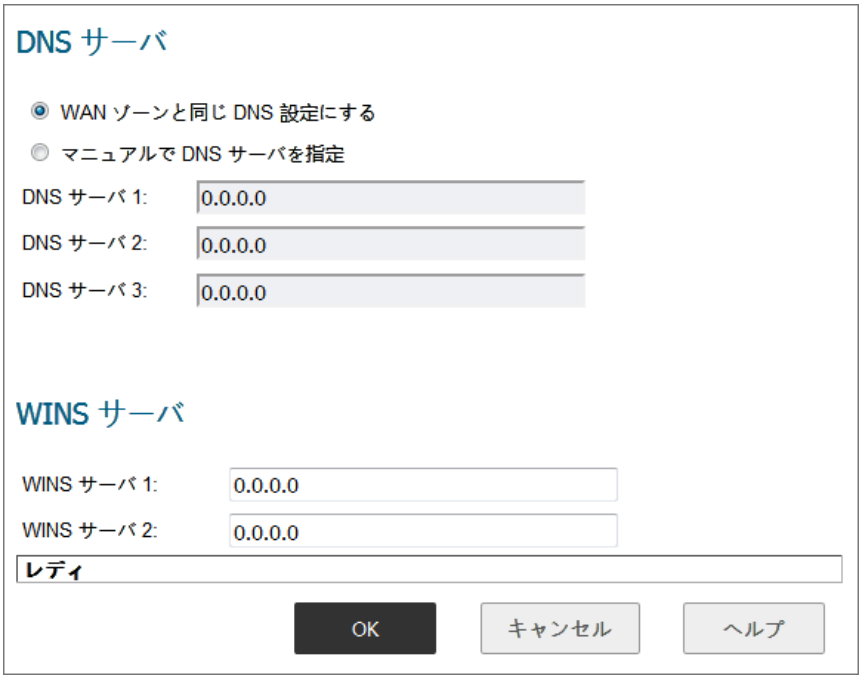
- **断片化パケットの処理を有効にする** - "断片化された IPSec パケットが破棄された" という内容のログ メッセージが VPN ログ レポートに示される場合は、この機能を有効にします。VPN トンネルが確立されて動作状態になるまでは、選択しないでください。
  - **DF (Don’t Fragment: 断片化を行わない) ビットを無視する** - パケット ヘッダーの DF ビットを無視するには、このチェックボックスをオンにします。一部のアプリケーションでは、パケットの'断片化を行わない'のオプションを明示的に設定できます。 これにより、すべてのセキュリティ装置にそのパケットの断片化を行わないように指示されます。このオプションが有効になっていると、ファイアウォールは断片化を行わないためのオプションを無視し、とにかくパケットの断片化を行います。
- **NAT トラバーサルを有効にする** - VPN エンドポイントの間に NAT 機器がある場合は、この設定を選択します。IPsec VPN は、認証されたエンドポイント間で交換されたトラフィックを保護しますが、NAT トラバーサルを動作させるために、認証されたエンドポイントをセッションの途中で動的に再マップできません。したがって、IPSec セッションが終了するまで動的な NAT バインドを維持するには、1 バイトの UDP を"NAT トラバーサル キープアライブ"として指定し、NAT 機器または NAPT 機器の背後にある VPN 機器によって送信される"ハートビート"として機能させます。"キープアライブ"は、IPsec peer により何も表示されずに破棄されます。
- **ピア ゲートウェイ DNS 名が別の IP アドレスに解決された時、アクティブなトンネルを一掃する** - 古い IP アドレスと関連付けられた SA を切断し、ピア ゲートウェイに再接続します。
- **「OCSP 確認を有効にする」および「OCSP 確認用 URL」** - VPN 証明書状況を確認する OCSP (Online Certificate Status Protocol) の使用を有効にし、証明書状況を確認する URL を指定します。「OCSP を SonicWall ネットワーク セキュリティ装置で使用」を参照してください。
- **トンネルの状況が変更した場合のみ、VPN トンネル トラップを送信する** - トンネルの状況が変化したときにのみトラップを送信することにより、送信される VPN トンネル トラップの数を減らします。
- **RADIUS を以下のモードで使用する** - このオプションを選択する主な理由は、VPN クライアント ユーザが MSCHAP 機能を使用して、ログイン時に期限切れパスワードを変更できるようにするためです。VPN クライアント ユーザの認証に RADIUS を使用する場合は、RADIUS を次のどちらのモードで使用するかを選択します。
  - **MSCHAP**
  - **MSCHAPv2** XAUTH のモード (期限切れパスワードの変更を可能にする)

  また、これを設定し、「**ユーザ > 設定**」ページの「**ログインの認証方法**」として LDAP が選択されているが、LDAP がパスワードの更新を許可する設定になっていない場合、LDAP を使用してユーザ認証が行われた後で、MSCHAP モードの RADIUS を使用して VPN クライアント ユーザのパスワードの更新が実行されます。

  メモ：次のいずれかを使用する場合のみ、LDAP によるパスワードの更新が可能です。
  - アクティブ ディレクトリを TLS と共に使用して、管理アカウントを使ってそれにバインドしている
  - ノベル イーディレクトリ

- **VPN クライアントの DNS および WINS サーバ設定** - GroupVPN を介したサードパーティ VPN クライアントや、モバイル IKEv2 クライアントなど、クライアント用に DNS および WINS サーバを設定するには、**設定**ボタンを選択します。「**VPN DNS および WINS サーバの追加**」ダイアログが表示されます。

  メモ：このオプションは、TZ 装置に対してのみ表示されます。



  - **DNS サーバ** - DNS サーバを動的に指定するか、手動で指定するかを選択します。
    - **WAN ゾーンと同じ DNS 設定にする** - SonicWall 装置は、DNS サーバ IP アドレスを自動的に取得します。
    - **マニュアルで DNS サーバを指定** -「**DNS サーバ 1/3**」フィールドに、DNS サーバ IP アドレスを最大 3 つ入力します。
  - **WINS サーバ** -「**WINS サーバ 1/2**」フィールドに、WINS サーバ IP アドレスを最大 2 つ入力します。

IKEv2 の設定

「**IKEv2 設定**」は、IKE 通知に影響を与え、動的クライアント サポートの設定が可能です。

- **IKEv2 Cookie 通知を送信する** - 認証ツールとして cookie を IKEv2 ピアに送信します。
- **IKEv2 の無効 SPI 通知を送信する** - アクティブな IKE SA (セキュリティ アソシエーション) が存在する場合に、無効な SPI (Security Parameter Index) 通知を IKEv2 ピアに送信します。このオプションは、既定では選択されています。
- **IKEv2 動的クライアント プロポーザル** - SonicOS は IKEv2 動的クライアントをサポートします。これにより、既定の設定を使用する代わりに、インターネット鍵交換 (IKE) 属性を設定できます。

  「**設定**」ボタンを選択すると、「**IKEv2 プロポーザル**」ダイアログが表示されます。

SonicOS は、以下の「**IKE プロポーザル**」設定をサポートします。

- **DH グループ**: **グループ 1**、**グループ 2** (既定)、**グループ 5**、**グループ 14**、および Suite B 暗号化に含まれる以下の 5 つの Diffie Hellman グループ。
  - **256 ビット ランダム ECP グループ**
  - **384 ビット ランダム ECP グループ**
  - **521 ビット ランダム ECP グループ**
  - **192 ビット ランダム ECP グループ**
  - **224 ビット ランダム ECP グループ**
- **暗号化**: **DES**、**3DES** (既定)、**AES-128**、**AES-192**、**AES-256**
- **認証**: **MD5**、**SHA1** (既定)、**SHA256**、**SHA384**、または **SHA512**

ただし、IKEv2 交換モードを使用する VPN ポリシーが定義され、0.0.0.0 の IPsec ゲートウェイが定義されている場合、個々のポリシーごとにこれらの IKE プロポーザル設定を行うことはできません。

メモ：リモート ゲートウェイの VPN ポリシーでも同じ設定を使用する必要があります。

OCSP を SonicWall ネットワーク セキュリティ装置で使用

OCSP は、PKI (Public Key Infrastructure) またはデジタル証明書システムで CRL を拡張または置換できるように設計されています。CRL は、PKI によって構成されたデジタル証明書の検証に使用されます。これにより、CA (証明書認証機関) は、予定された有効期限になる前に証明書を取り消します。 これは、盗まれた証明書や無効な証明書に対して PKI を保護する場合に有用です。

証明書失効リストの主な短所は、各クライアントの CRL を最新にしておくためにアップデートを頻繁に行うことが必要な点です。頻繁なアップデートが必要になると、各クライアントで完全な CRL がダウンロードされるときにネットワーク トラフィックが増大します。CRL アップデートの頻度によっては、CRL によって証明書が取り消された時点でクライアントが CRL アップデートおよび証明書の使用の許可をまだ入手していないという状態が、一定の期間にわたって発生することがあります。

Online Certificate Status Protocol は、CRL を使用せずにデジタル証明書の現在の状況を判断します。OCSP は、識別されたデジタル証明書の状況をクライアントまたはアプリケーションが直接判断できるようにします。これにより、CRL 証明書に関する情報を CRL の場合よりも適切なタイミングで提供

できます。さらに、通常は各クライアントがいくつかの証明書を確認するだけなので、いくつかのエントリのために CRL 全体をダウンロードしてもオーバーヘッドは発生しません。その結果、証明書の検証に関連するネットワーク トラフィックが大幅に減少します。

OCSP は、既存のネットワークとの互換性を最大化するためにメッセージを HTTP 経由で転送します。そのため、OCSP 応答のキャッシュされたコピー (期限切れの可能性がある) を受け取らないように、ネットワーク内のキャッシュ サーバを慎重に設定する必要があります。

OCSP クライアントは、OCSP レスポンダでやり取りします。OCSP レスポンダは、CA サーバまたは CA とやり取りして証明書状況を判断できる他のサーバにすることができます。OCSP クライアントは、OCSP レスポンダに状況要求を発行し、レスポンダから応答があるまで証明書の受け入れを保留します。クライアント要求には、プロトコル バージョン、サービス要求、ターゲット証明書 ID、オプションの拡張機能などのデータが含まれています。オプションの拡張は、OCSP レスポンダによって承認されない場合もあります。

OCSP レスポンダは、クライアントから要求を受け取ると、メッセージが適切な形式であることを確認し、レスポンダがサービス要求に応答できるかどうかを検証します。次に、要求の中に目的のサービスに必要な情報が正しく含まれているかを確認します。すべての条件が満たされると、レスポンダは OCSP クライアントに最終的な応答を返します。OCSP レスポンダは、基本的な応答 (GOOD、REVOKED、または UNKNOWN) を提供する必要があります。OCSP クライアントとレスポンダが両方ともオプションの拡張をサポートしている場合は、他の応答も可能です。GOOD 状態は、証明書が取り消されていないことを示す、期待されている応答です。REVOKED 状態は、証明書が取り消されたことを示します。UNKNOWN 状態は、レスポンダが対象となる証明書に関する情報を持っていないことを示します。

OCSP サーバは、通常、プッシュまたはプル設定で CA サーバと連携して動作します。CRL リスト (証明書失効リスト) を OCSP サーバにプッシュするように CA サーバを設定できます。さらに、OCSP サーバは、CA サーバから CRL を周期的にダウンロード (プル) するように設定できます。OCSP サーバは、CA サーバで発行された OCSP 応答署名証明書によって設定することもできます。署名証明書は適切な形式である必要があります。そうでない場合、OCSP クライアントは OSCP サーバからの応答を受け入れません。

OpenCA OCSP Responder

OCSP を使用するには、サポートされている唯一の OCSP レスポンダである、OpenCA (オープンソース証明書認証機関) の OpenCA OCSP Responder が必要です。OpenCA OCSP Responder は、http://www.openca.org で入手できます。OpenCA OCSP Responder は、rfc2560 に準拠した OCSP レスポンダであり、既定のポート 2560 (rfc2560 に基づくことを示す) で動作します。

OCSP で使用する証明書のロード

SonicOS がレスポンダに対して OCSP クライアントとして動作するように設定する場合は、CA 証明書をファイアウォールにロードする必要があります。

1 「**システム** > **証明書**」ページで、「**インポート**」ボタンを選択します。「**証明書のインポート**」ページが表示されます。

2 「**PKCS#7 (.p7b)、PEM (.pem)、DER (.der か .cer) エンコード ファイルから、CA 証明書をインポートする**」オプションを選択し、証明書の場所を指定します。

OCSP で VPN ポリシーを使用

ファイアウォール OCSP 設定は、ポリシー レベルで、またはグローバルに設定できます。個別の VPN ポリシーで OCSP 確認を設定するには、「VPN ポリシー」設定ページの「詳細」タブを使用します。

1 「**OCSP 確認を有効にする**」の隣にあるチェックボックスを選択します。

2 OCSP サーバの「**OCSP 確認用 URL**」を指定します。例えば、http://192.168.168.220:2560 とした場合、"192.168.168.220" は OCSP サーバの IP アドレスで、"2560" は OpenCA OCSP レスポンダ サービスの動作の既定ポートです。

6

VPN を越えた DHCP の設定

「**VPN > VPN を越えた DHCP**」ページでは、ファイアウォールを設定して、VPN トンネルの反対側にある DHCP サーバから IP アドレス リースを取得できます。ネットワークの配備によっては、1 つの論理 IP アドレス上にすべての VPN ネットワークを配置し、1 つの IP サブネット アドレス スペースに存在するすべての VPN ネットワークの外観を作成するのが望ましい場合があります。これにより、VPN トンネルを使用するネットワークの IP アドレス管理が容易になります。

トピック:

- DHCP リレー モード
- VPN を越えた DHCP 用のセントラル ゲートウェイの設定
- VPN を越えた DHCP のリモート ゲートウェイの設定
- VPN を越えた現在の DHCP リース

DHCP リレー モード

リモート サイトおよび中央サイトのファイアウォールは、サイト間の最初の DHCP トラフィックおよびそれ以降の IP トラフィックに対して、VPN トンネル用に設定されます。リモート サイトのファイアウォール (**リモート ゲートウェイ**) は、VPN トンネルを通して DHCP ブロードキャスト パケットを渡します。中央サイトのファイアウォール (**セントラル ゲートウェイ**) は、リモート ネットワーク上のクライアントからの DHCP パケットを、中央サイトの DHCP サーバにリレーします。

VPN を越えた DHCP 用のセントラル ゲートウェイの設定

セントラル ゲートウェイに VPN を越えた DHCP を設定するには、以下の手順を使用します。

1 「**VPN > VPN を越えた DHCP**」を選択します。

2 「**VPN を越えた DHCP**」ドロップダウン メニューから「**セントラル ゲートウェイ**」を選択します。

3 「**設定**」を選択します。

4 次のいずれかを選択します。

- グローバル VPN クライアント向け、リモート ファイアウォール向け、またはその両方に対して DHCP サーバを使用する場合は、「**内部 DHCP サーバを使用する**」オプションを選択します。
    - グローバル VPN クライアント向けに DHCP サーバを使用する場合は、「**グローバル VPN クライアント向け**」オプションを選択します。
    - リモート ファイアウォール向けに DHCP サーバを使用する場合は、「**リモート ファイアウォール向け**」オプションを選択します。
- 特定のサーバに DHCP リクエストを送信する場合は、「**下記にリストされたサーバ IP アドレスに DHCP リクエストを送信する**」を選択します。
    a) 「**追加**」を選択します。
    b) 「**IP アドレス**」フィールドに DHCP サーバの IP アドレスを入力します。

c) 「**OK**」を選択します。指定したサーバにファイアウォールが DHCP リクエストを送信するようになります。

5 「**リレー IP アドレス (オプション)**」フィールドに、リレー サーバの IP アドレスを入力します。

この IP アドレスを設定した場合、これが DHCP リレー エージェント IP アドレス (giaddr) として、この SonicWall の LAN IP アドレスの代わりに使用されます。この IP アドレスは、リモート ゲートウェイ上にリレー IP アドレスが設定されていない場合のみ使用されます。また、DHCP サーバ上の DHCP スコープ内で予約されている必要があります。

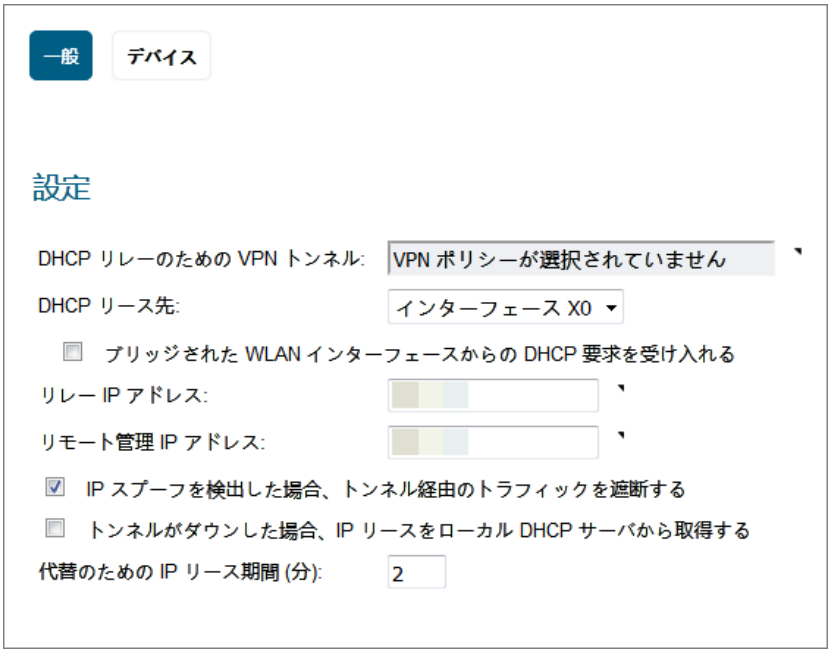
6 「**OK**」を選択します。

VPN を越えた DHCP のリモート ゲートウェイの設定

VPN を越えた DHCP のリモート ゲートウェイを設定するには、以下の手順に従います。

1 「**VPN を越えた DHCP**」ドロップダウン メニューから「**リモート ゲートウェイ**」を選択します。

2 「**設定**」を選択します。



3 VPN ポリシーで「**ローカル ネットワークは、この VPN トンネルを通じた DHCP を使用して IP アドレスを取得する**」設定が有効になっている場合は、「**一般**」画面の「**DHCP リレーのための VPN トンネル**」フィールドに、VPN ポリシー名が自動的に表示されます。

メモ：IKE を使用する VPN ポリシーのみが DHCP の VPN トンネルとして使用できます。VPN トンネルは IKE を使用する必要があり、ローカル ネットワークは適切に設定されている必要があります。ローカル ネットワークは、この VPN トンネルを通じた DHCP を使用して IP アドレスを取得します。

4 「**DHCP リース先**」メニューから DHCP リース先となるインターフェースを選択します。

5 ブリッジされた WLAN インターフェースからの DHCP 要求を受け入れる場合は、「**ブリッジされた WLAN インターフェースからの DHCP 要求を受け入れる**」チェックボックスをオンにします。

6 「**リレー IP アドレス**」フィールドに IP アドレスを入力すると、この IP アドレスはセントラル ゲートウェイのアドレスの代わりに DHCP リレー エージェント アドレス (giaddr) として使用されます。また、DHCP サーバ上の DHCP スコープ内で予約されている必要があります。このアドレスは、セントラル ゲートウェイの背後にある VPN トンネルを通して、このファイアウォールをリモートで管理するためにも使用できます。

> **メモ**：トンネルを通した管理が必要な場合は、「リレー IP アドレス」と「リモート管理 IP アドレス」のフィールドをゼロにすることはできません。

7 「**リモート管理 IP アドレス**」フィールドに IP アドレスを入力すると、この IP アドレスは、セントラル ゲートウェイの背後からファイアウォールを管理するために使用されます。また、DHCP サーバ上の DHCP スコープ内で予約されている必要があります。

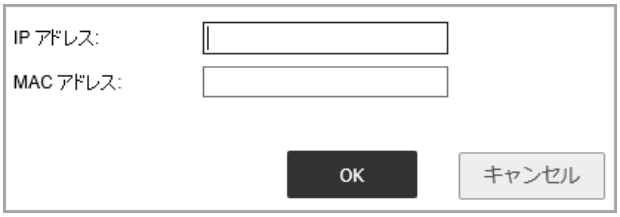
8 「**IP スプーフを検出した場合、トンネル経由のトラフィックを遮断する**」を有効にすると、ファイアウォールは、認証されたユーザの IP アドレスになりすます、VPN トンネル経由のトラフィックを遮断します。ただし、固定の機器がある場合は、機器に対して正しいイーサネット アドレスが入力されていることを確認する必要があります。イーサネット アドレスは識別プロセスの一部として使用され、イーサネット アドレスが正しくないと、ファイアウォールが IP Spoof として応答する可能性があります。

9 VPN トンネルが中断された場合は、一時的な DHCP リースをローカル DHCP サーバから取得できます。トンネルが再びアクティブになると、ローカル DHCP サーバはリースの発行を停止します。「**トンネルがダウンした場合、IP リースをローカル DHCP サーバから取得する**」チェックボックスをオンにします。このチェック ボックスをオンにすることで、トンネルが機能を停止するときのフェイルオーバー オプションになります。

10 一定の時間だけ一時的なリースを許可する場合は、「**代替のための IP リース期間 (分)**」ボックスに一時リースの分数を入力します。既定値は **2** 分です。

11 LAN の機器を設定するには、「**デバイス**」を選択します。

12 「**静的な LAN デバイス**」を設定するには、「**追加**」を選択して「**静的な LAN デバイスの追加**」ダイアログを表示します。



13 「**IP アドレス**」フィールドに機器の IP アドレスを入力し、「**MAC アドレス**」フィールドにイーサネット アドレスを入力します。

静的な機器の例としては、IP リースを動的に取得できないプリンタなどがあります。「**IP スプーフを検出した場合、トンネル経由のトラフィックを遮断する**」を有効にしてない場合は、機器のイーサネット アドレスを入力する必要はありません。DHCP サーバで利用可能な IP アドレスのプールから静的 IP アドレスを除外して、DHCP サーバがこれらのアドレスを DHCP クライアントに割り当てないようにする必要があります。また、**リレー IP アドレス**として使用される IP アドレスも除外する必要があります。リレー IP アドレスとして使用する IP アドレスを遮断することをお勧めします。

14 「**OK**」を選択します。

15 LAN 上の機器を除外するには、「**追加**」を選択して「**除外する LAN デバイスの追加**」ダイアログを表示します。

16 「**MAC アドレス**」フィールドに、機器の MAC アドレスを入力します。

17 「**OK**」を選択します。

18 「**OK**」を選択して、「**VPN を越えた DHCP/リモート ゲートウェイ**」ダイアログを閉じます。

メモ：コンピュータに IP リースを割り当てるには、リモート ファイアウォール上にローカル DHCP サーバを設定する必要があります。

メモ：リモート サイトでセントラル ゲートウェイへの接続およびリースの取得に関する問題がある場合は、リモート コンピュータで Deterministic Neteork Enhancer (DNE) が有効になっていないことを確認します。

ヒント：例えば 2 つの LAN のように、静的 LAN IP アドレスが DHCP スコープの外部にある場合は、この IP へのルーティングが可能です。

VPN を越えた現在の DHCP リース

「**VPN を越えた現在の DHCP リース**」テーブルは、現在のバインドに関する詳細情報として、**IP アドレス**、**ホスト名**、**MAC アドレス**、**リース期間**、および**トンネル名**を表示します。テーブルの最後の列にある「**設定**」により、テーブル エントリ (バインド) を設定または削除できます。

- バインドを編集するには、「**編集**」を選択します。
- バインドを削除するには、リストからバインドを選択し、**削除**アイコンを選択します。バインドを削除すると、DHCP サーバで IP アドレスが解放されます。操作が完了するまで数秒かかります。完了すると、ウェブ ブラウザ ウィンドウの一番下に更新を確認するメッセージが表示されます。
- すべての VPN リースを削除するには、「**すべて削除**」を選択します。

7

L2TP サーバと VPN クライアント アクセスの設定

SonicWall ネットワーク セキュリティ装置では、Microsoft Windows または Google Android 着信クライアントからの L2TP-over-IPsec 接続を切断できます。グローバル VPN クライアント (GVC) を実行できない状況において、SonicWall L2TP サーバを使用し、ファイアウォールの背後にあるリソースへの安全なアクセスを提供できます。

レイヤ 2 トンネリング プロトコル (L2TP) を使用すると、パブリック ネットワークに VPN を作成できます。L2TP は、PPTP や L2F などの相互運用性のないプロトコルを使用する異なる VPN の間の相互運用性を提供します。

L2TP は、Microsoft Windows 2000 オペレーティング システムでサポートされます。L2TP は、パスワード認証プロトコル (PAP)、チャレンジ ハンドシェイク認証プロトコル (CHAP)、Microsoft チャレンジ ハンドシェイク認証プロトコル (MS-CHAP) など、PPP がサポートする複数の認証オプションをサポートします。

トピック:

メモ：L2TP サーバの設定の詳細については、次の SonicOS サポート サイトにある TechNote 『**Configuring the L2TP Server in SonicWall**』を参照してください: https://www.sonicwall.com/ja-jp/support。

L2TP サーバの設定

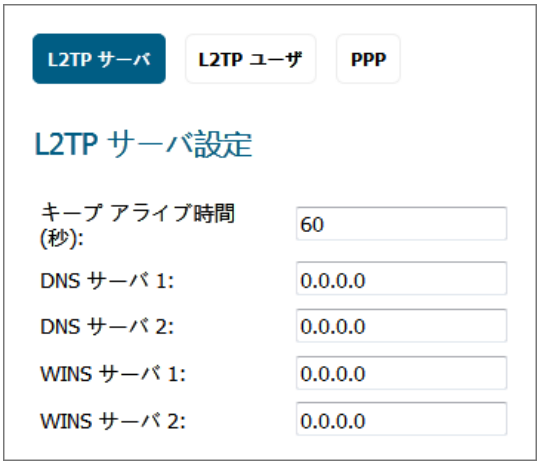
「**管理 | 接続性 | VPN > L2TP サーバ**」ページに、SonicWall ネットワーク セキュリティ装置を L2TP サーバとして設定するための項目があります。

L2TP サーバを設定するには、以下の手順に従います。

1 「**管理 | 接続性 | VPN > L2TP サーバ**」ページに移動します。

2 「**L2TP サーバを有効にする**」チェックボックスをオンにします。「**設定**」が使用可能になります。

3 「**設定**」を選択して、「**L2TP サーバ設定**」ダイアログを表示します。

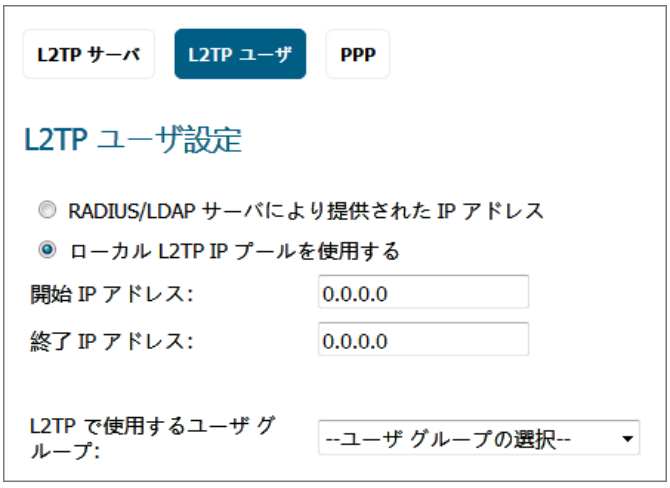


4 「**L2TP サーバ**」画面の「**キープ アライブ時間 (秒)**」フィールドに秒数を入力します。この値は、接続を開いておくための特殊なパケットを送信する頻度を指定するものです。既定値は **60** 秒です。

5 第 1 の DNS サーバの IP アドレスを、「**DNS サーバ 1**」フィールドに入力します。第 2 の DNS サーバがある場合は、その IP アドレスを「**DNS サーバ 2**」フィールドに入力します。

6 第 1 の WINS サーバの IP アドレスを、「**WINS サーバ 1**」フィールドに入力します。第 2 の WINS サーバがある場合は、その IP アドレスを「**WINS サーバ 2**」フィールドに入力します。

7 「**L2TP ユーザ**」を選択します。



8 IP アドレス設定で次のいずれかのラジオ ボタンを選択します。

RADIUS/LDAP サーバにより提供された IP アドレス	既定では、このオプションはオフになっています。RADIUS/LDAP サーバが L2TP クライアントに IP アドレス情報を提供する場合にこれを選択します。「**開始 IP アドレス**」フィールドと「**終了 IP アドレス**」フィールドがアクティブではなくなります。 **メモ**：このオプションを使用するためには、「**管理 | システム セットアップ | ユーザ > 設定**」ページで、RADIUS もしくは LDAP 認証が選択されている必要があります。このオプションを選択すると、この趣旨の情報メッセージが表示されます。「**OK**」を選択します。
ローカル L2TP IP プールを使用する	このオプションは既定の IP アドレス設定です。L2TP サーバが IP アドレスを提供する場合はこれを選択します。 LAN のプライベート IP アドレスの範囲を、「**開始 IP アドレス**」フィールドと「**終了 IP アドレス**」フィールドに入力します。

9 L2TP を使用するために定義された特定のユーザ グループを設定済みである場合は、「**L2TP で使用するユーザ グループ**」メニューからそのグループを選択するか、「**Everyone**」を使用します。

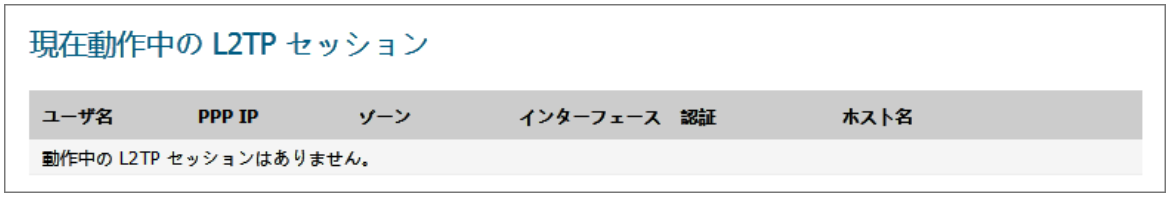
10 「**PPP**」を選択します。

11 認証プロトコルを選択し、「**追加**」を選択して追加します。認証プロトコルを削除したり、認証の順序を並べ替えたりすることもできます。

12 「**OK**」を選択します。

現在動作中の L2TP セッションの表示

「**動作中の L2TP セッション**」セクションには、現在動作中の L2TP セッションが表示されます。



以下の情報が表示されます。

ユーザ名	ローカル ユーザ データベースまたは RADIUS ユーザ データベースで割り当てられているユーザ名。
PPP IP	接続のソース IP アドレス。
ゾーン	L2TP クライアントにより使用されるゾーン。
インターフェース	VPN クライアントまたは別のファイアウォールのどちらでも、L2TP サーバへのアクセスに使用されるインターフェース。
認証	L2TP クライアントが使用する認証の入力。
ホスト名	L2TP サーバに接続している L2TP クライアントの名前。

Microsoft Windows L2TP VPN クライアント アクセスの設定

このセクションでは、組み込みの L2TP サーバと Microsoft の L2TP VPN クライアントを使用して WAN GroupVPN SA への L2TP クライアント アクセスを設定するための例を示します。

メモ：SonicOS は、L2TP クライアントに対して X.509 証明書のみをサポートします。PKCS #7 エンコードの X.509 証明書は、SonicOS において L2TP 接続に対してサポートされていません。

WAN GroupVPN SA への Microsoft L2TP VPN クライアント アクセスを有効にするには、以下の手順に従います。

1 「**管理 | 接続性 | VPN > 基本設定**」ページに移動します。

2 WAN GroupVPN ポリシーについては、「**設定**」列で「**編集**」アイコンを選択します。

3 「**一般**」画面の「**認証方式**」で、「**IKE (事前共有鍵を使用)**」を選択します。

4 「**事前共有鍵**」フィールドに事前共有鍵のパスフレーズを入力して、クライアント ポリシーの設定を完了します。

5 「**OK**」を選択します。

6 「**管理 | 接続性 | VPN > L2TP サーバ**」ページに移動します。

7 「**L2TP サーバ設定**」セクションで、「**L2TP サーバを有効にする**」チェックボックスをオンにします。

8 「**設定**」を選択します。

9 次の L2TP サーバ設定を指定します。

- **キープ アライブ時間 (秒)**: *60*
- **DNS サーバ 1**: *199.2.252.10* (または ISP の DNS を使用)
- **DNS サーバ 2**: *4.2.2.2* (または ISP の DNS を使用)
- **DNS サーバ 3**: *0.0.0.0* (または ISP の DNS を使用)
- **WINS サーバ 1**: *0.0.0.0* (または独自の WINS の IP を使用)
- **WINS サーバ 2**: *0.0.0.0* (または独自の WINS の IP を使用)

10 「**L2TP ユーザ**」を選択します。

11 以下のオプションを設定します。

- **ローカル L2TP IP プールを使用する**: 有効 (選択状態。既定)
- **開始 IP アドレス**: *10.20.0.1* (自分の IP を使用する)
- **終了 IP アドレス**: *10.20.0.20* (自分の IP を使用する)

12 「**L2TP で使用するユーザ グループ**」ドロップダウン メニューから「**Trusted Users**」を選択します。

13 「**OK**」を選択します。

14 「**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**」ページに移動します。

15 「**ローカル ユーザ**」を選択します。

16 「**追加**」を選択して「**ユーザ設定**」ダイアログを表示します。

17 「**名前**」、「**パスワード**」、「**パスワードの確認**」のフィールドに、ユーザ名とパスワードを指定します。

18 「**OK**」を選択します。

> **メモ**：VPN > LAN アクセス ルールまたは別の VPN アクセスルール（「**管理 | ポリシー | ルール > アクセス ルール**」の下）を編集することにより、L2TP クライアントのネットワーク アクセスを制限できます。編集対象のルールを見つけるには、「**アクセス ルール**」テーブルの「**表示: すべての種別**」を選択し、「**L2TP IP プール**」の「送信元」列に着目します。

19 Microsoft Windows コンピュータ上で、次の L2TP VPN クライアント設定を完了して、安全なアクセスを有効にします。

a 「**スタート > コントロール パネル > ネットワークと共有センター**」に移動します。

b 新しい接続ウィザードを開きます。

c 「**職場に接続**」を選択します。

d 「**次へ**」ボタンを選択します。

e 「**仮想プライベート ネットワーク接続**」を選択します。「**次へ**」ボタンを選択します。

f VPN 接続の名前を入力します。「**次へ**」ボタンを選択します。

g ファイアウォールのパブリック (WAN) IP アドレスを入力します。ファイアウォールを指すドメイン名を使用することもできます。

h 「**次へ**」を選択し、「**完了**」を選択します。

i 「接続」ウィンドウで「**プロパティ**」を選択します。

j 「**セキュリティ**」を選択します。

k 「**IPSec 設定**」を選択します。

l 「**認証に事前共有キーを使う**」を有効にします。

m 事前共有鍵を入力し、「**OK**」を選択します。

n 「**ネットワーク**」を選択します。

o 「**VPN の種類**」を「**自動**」から「**L2TP IPsec VPN**」に変更します。

p 「**OK**」を選択します。

q XAUTH ユーザ名およびパスワードを入力します。

r 「**接続**」を選択します。

20 「**管理 | 接続性 | VPN > 基本設定**」ページに移動して、Microsoft Windows L2TP VPN デバイスが接続されていることを確認します。VPN クライアントが「**現在アクティブな VPN トンネル数**」セクションに表示されます。

Google Android L2TP VPN クライアント アクセスの設定

このセクションでは、組み込みの L2TP サーバと Google Android の L2TP VPN クライアントを使用して WAN GroupVPN SA への L2TP クライアント アクセスを有効にするための設定例を示します。

WAN GroupVPN SA への Google Android L2TP VPN クライアント アクセスを有効にするには、次の手順に従います。

1 「**管理 | 接続性 | VPN > 基本設定**」ページに移動します。

2 WAN GroupVPN ポリシーに対しては、「**編集**」アイコンを選択します。

3 「**認証方式**」ドロップダウン メニューから「**IKE (事前共有鍵を使用)**」 (既定) を選択します。

4 「**事前共有鍵**」フィールドに事前共有鍵のパスフレーズを入力して、クライアント ポリシーの設定を完了します。

5 「**プロポーザル**」を選択します。

6 「**IKE (フェーズ 1) プロポーザル**」で、以下のように設定します。

- DH グループ: **グループ 2**
- 暗号化: **3DES**
- 認証: **SHA1**

- 存続期間 (秒): **28800**

7 「**IPsec (フェーズ 2) プロポーザル**」で、以下のように設定します。

- プロトコル: **ESP**
- 暗号化: **DES**
- 認証: **SHA1**
- Perfect Forward Secrecy を有効にする: **有効**
- 存続期間 (秒): **28800**

8 「**詳細設定**」を選択します。

9 以下のオプションを設定します。

- **マルチキャストを有効にする**: 無効
- **この SA を経由しての管理**: すべて無効
- **デフォルト ゲートウェイ**: 0.0.0.0
- **XAUTH を利用した VPN クライアントの認証を要求する**: 有効
- **XAUTH に使用するユーザ グループ**: Trusted Users

10 「**クライアント**」を選択します。

11 以下のオプションを設定します。

- **XAUTH ユーザ名とパスワードのクライアント キャッシュ**: セッション単位または常に有効
- **仮想アダプターの設定**: DHCP リース
- **コネクションの制御**: Split Tunnels
- **このゲートウェイをデフォルト ルートに設定する**: 無効
- **VPN アクセス制御リストを適用する**: 無効
- **シンプル クライアント プロビジョニングに既定の鍵を使用する**: 有効

12 「**OK**」を選択します。

13 「**管理 | 接続性 | VPN > L2TP サーバ**」ページに移動します。

14 「**L2TP サーバを有効にする**」チェックボックスをオンにします。

15 「**設定**」を選択します。

16 次の L2TP サーバ設定を指定します。

- **キープ アライブ時間 (秒)**: 60
- **DNS サーバ 1**: 199.2.252.10 (または ISP の DNS を使用)
- **DNS サーバ 2**: 4.2.2.2 (または ISP の DNS を使用)
- **DNS サーバ 3**: 0.0.0.0 (または ISP の DNS を使用)
- **WINS サーバ 1**: 0.0.0.0 (または独自の WINS の IP を使用)
- **WINS サーバ 2**: 0.0.0.0 (または独自の WINS の IP を使用)

17 「**L2TP ユーザ**」を選択します。

18 以下のオプションを設定します。

- **RADIUS/LDAP サーバにより提供された IP アドレス**: 無効
- **ローカル L2TP IP プールを使用する**: 有効
- **開始 IP アドレス**: 10.20.0.1 (または自分のものを使用)
- **終了 IP アドレス**: 10.20.0.20 (または自分のものを使用)

19 「**L2TP で使用するユーザ グループ**」ドロップダウン メニューで、「**Trusted Users**」を選択します。

20 「**OK**」を選択します。

21 「**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**」ページに移動します。

22 「**ローカル ユーザ**」を選択します。

23 「**追加**」を選択します。

24 「**管理 | システム セットアップ | ユーザ > ローカル ユーザ**」ページに移動します。「**ユーザの追加**」ボタンを選択します。

25 「**設定**」画面で、ユーザ名とパスワードを指定します。

26 「VPN アクセス」タブで、希望するネットワーク アドレス オブジェクトを追加します。これらのオブジェクトによって L2TP クライアントはアクセス リストのネットワークに関連付けられます。

> **メモ**：少なくとも、LAN サブネット、LAN プライマリ サブネット、および L2TP IP プール アドレス オブジェクトをアクセス リストに追加します。

> **メモ**：これで、SonicOS 設定が完了しました。

27 Google Android デバイス上で、次の L2TP VPN クライアント設定を完了して、安全なアクセスを有効にします。

a APP ページに移動し、「**設定**」アイコンを選択します。「設定」メニューから「**無線およびネットワーク**」を選択します。

b 「**VPN 設定**」を選択し、「**VPN を追加**」を選択します。

c 「**L2TP/IPSec PSK VPN を追加**」を選択します。

d 「VPN 名」に VPN フレンドリ名を入力します。

e 「**VPN サーバ**」を設定します。

f ファイアウォールのパブリック IP アドレスを入力します。

g **IPSec 事前共有鍵を設定**: WAN グループ VPN ポリシーのパスフレーズを入力します。

h 「**L2TP 鍵**」は空白のままにします。

i 必要に応じて、LAN ドメイン設定を設定します。この設定はオプションです。

j XAUTH ユーザ名およびパスワードを入力します。「**接続**」を選択します。

28 「**管理 | 接続性 | VPN > 設定**」ページに移動して、Google Android デバイスが接続されていることを確認します。VPN クライアントが「現在アクティブな VPN トンネル数」セクションに表示されます。

8

AWS VPN

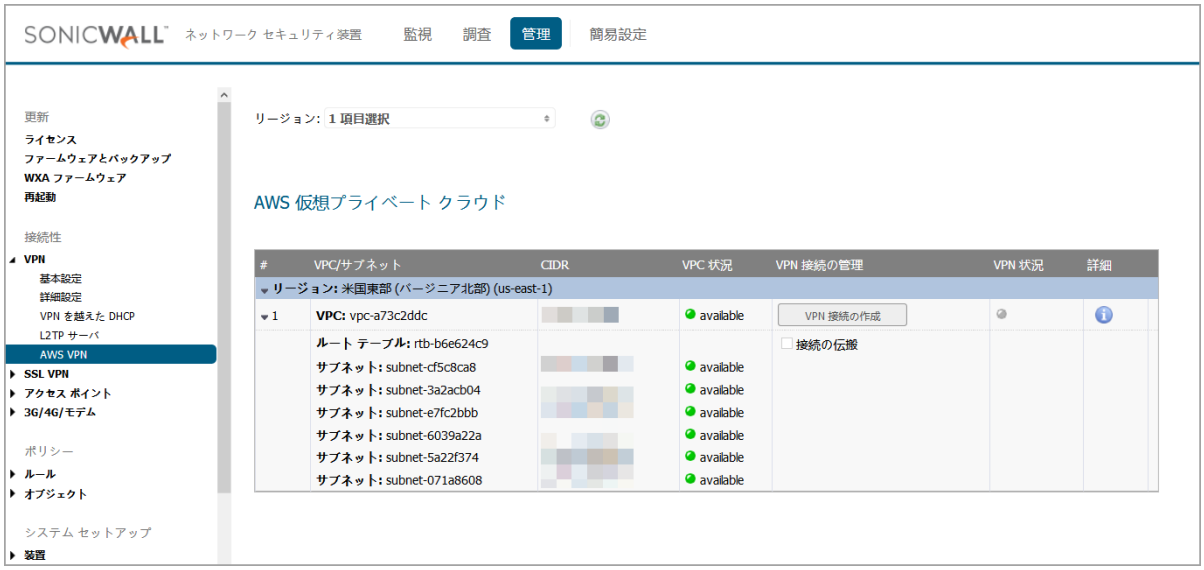
「AWS VPN」ページでは、SonicWall ファイアウォールから アマゾン ウェブ サービス (AWS) 上の仮想プライベート クラウド (VPC) への VPN 接続を簡単に作成できます。Amazon 仮想プライベート クラウドの詳細については、https://aws.amazon.com/vpc/ を参照してください。

重要： AWS VPN を設定する前に、そこで必要とされる AWS 資格情報を使用してファイアウォールを設定してください。これを行うには、「**管理**」ビューの「**システム セットアップ | ネットワーク > AWS 設定**」に移動します。さらに、「**設定のテスト**」を選択して、設定を確認してから作業を進めてください。

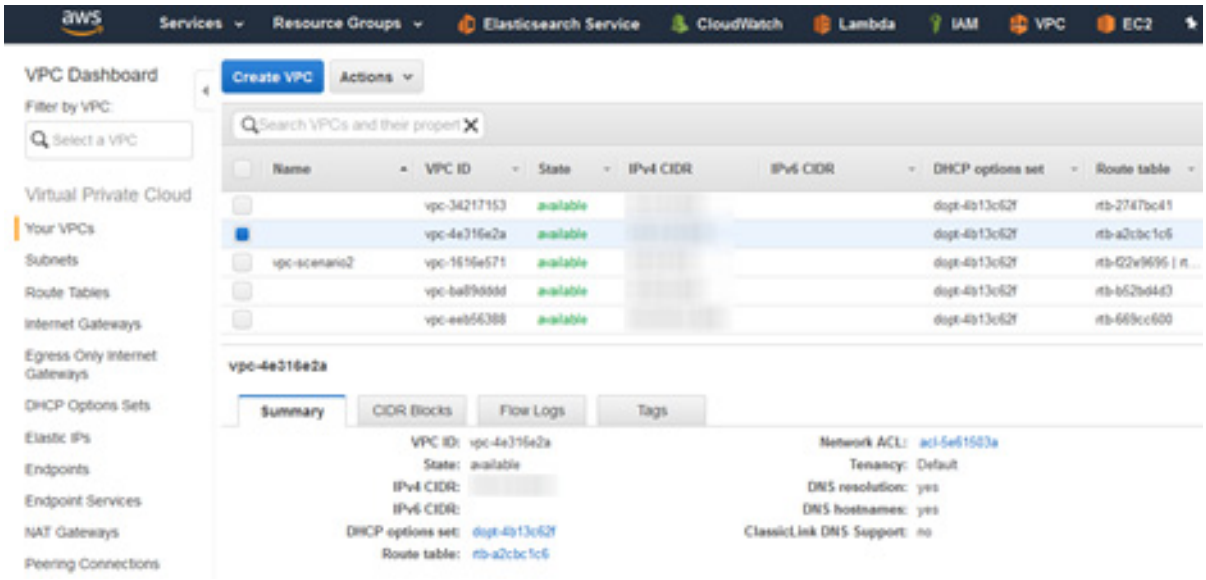
トピック:

概要

AWS VPN にアクセスするには、「**管理 | 接続性 > VPN > AWS VPN**」に移動します。「AWS VPN」ページの中心となる部分は、関心の対象とされている AWS リージョンの VPC を示すテーブルです。このテーブルの個々の行を展開して、VPC のサブネットを (ルート テーブルごとに整理して) 表示することができます。このテーブルには、ステータス情報を表示する列や、対応する VPC への VPN 接続を作成したり削除したりするためのボタンもあります。

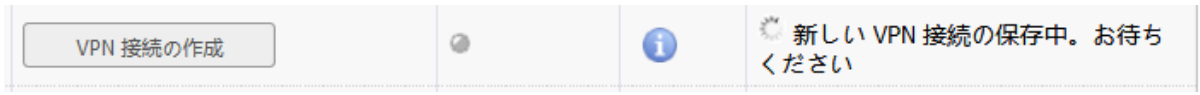


ファイアウォールの「AWS VPN」ページにあるこのテーブルは、AWS コンソール上の VPC ダッシュボードで使用可能な VPC 情報を示しています (以下を参照)。



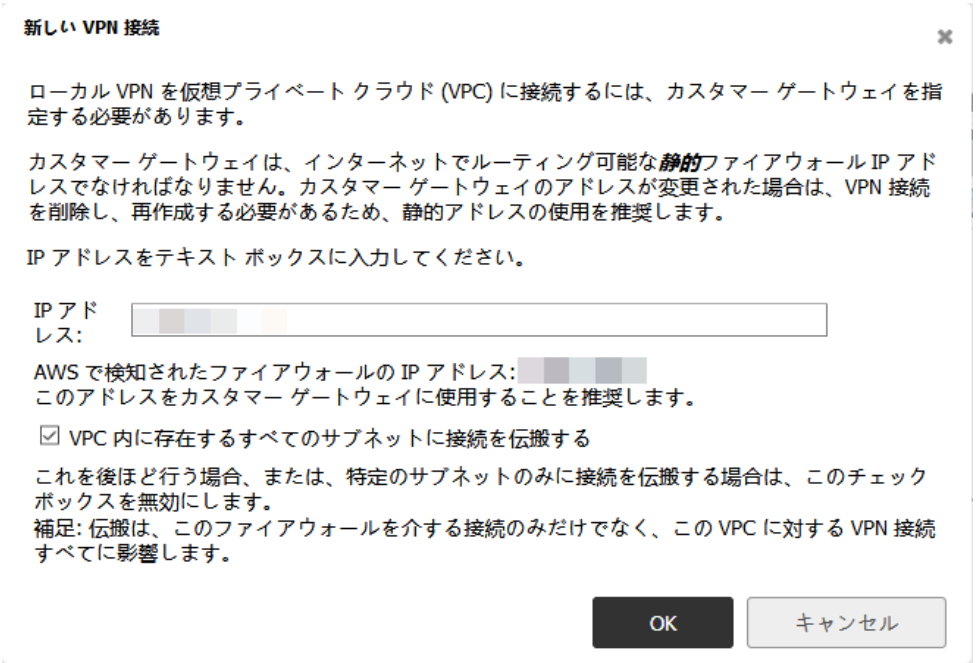
新しい VPN 接続の作成

ファイアウォールから新しい VPN 接続を作成するのは比較的簡単です。この処理を開始するには、ファイアウォールに接続したい Amazon VPC の該当する行の「**VPN 接続の作成**」ボタンをクリックします。



「**新しい VPN 接続**」ウィンドウが表示されます。AWS から見たファイアウォールのパブリック IP アドレスを指定します。AWS 上で実行されているコードが、アドレスを検出し、テキスト入力フィールドの値を事前に設定しようとします。ローカル ネットワークの外部から到達可能なアドレスである

ことを確認してください。ファイアウォールがルータまたはその他のプロキシの背後にある場合は、NAT ルールを適切に設定して、AWS 側から開始された VPN トラフィックが再びファイアウォールにルーティングされるようにしてください。



メモ：場合によっては、ルート伝搬を有効にするかどうかを尋ねられることがあります。詳細については、「経路伝搬」を参照してください。

入力した IP アドレスは、カスタマー ゲートウェイとして使用されます。「**OK**」を選択してダイアログを閉じ、ファイアウォールと AWS の両方を設定する一連のプロセスを開始し、それらの間の VPN 接続を確立します。

新しい VPN 接続の対象となる VPC のテーブル行にメッセージが表示され、さまざまな段階で進行状況が通知されます。

いずれかの段階でエラーが発生すると、問題の詳細を示すメッセージが表示され、それまでに行ったすべての変更が元に戻されます。その場合は、問題を解決してやり直してください。

VPN 接続の確認

ファイアウォールと AWS 上の VPC 間に新しいVPN 接続を作成した後、その過程でそれぞれの設定がどのように変更されたかを詳細に表示できます。

ファイアウォールで、「**管理 | 接続性 > VPN > AWS VPN**」に移動します。該当する AWS VPC に対応する VPC テーブルの行を探し、「**情報**」ボタンをクリックします。VPN 接続の詳細が表示されます。

メモ：VPN 接続が作成されたばかりであるため、ステータスは依然として**保留中**として報告されます。「AWS VPN」ページの「**再表示**」ボタンをクリックすると、テーブルのデータと、関連する「VPN 接続詳細」ウィンドウのデータが再ロードされます。

以下のセクションでは、ファイアウォールおよび AWS での設定について説明します。

- ファイアウォールでの設定
- アマゾン ウェブ サービスでの設定

ファイアウォールでの設定

新しい VPN 接続を作成する過程で、VPC を表すアドレス オブジェクトが追加されます。SonicOS では、これを「**アドレス オブジェクト**」ページで表示できます。「**管理 | ポリシー | オブジェクト > アドレス オブジェクト**」に移動します。このオブジェクトの命名規則によって、VPN 接続の AWS ID と VPC 自体の AWS ID が組み合わされます。このアドレス オブジェクトの種別はネットワークで、ネットワークはリモート VPC ネットワークのものです。

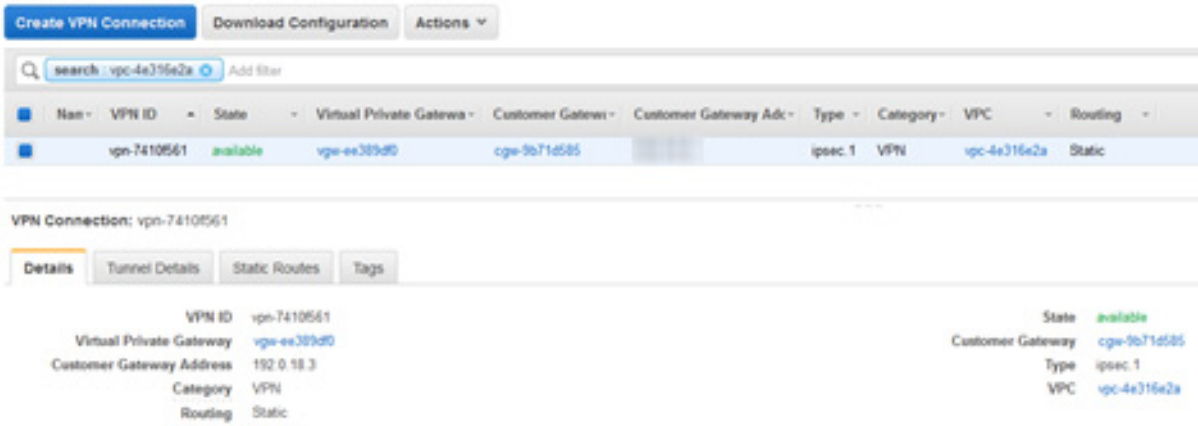
2 つの VPN ポリシーも作成されます。AWS が VPN 接続ごとに 2 つの VPN を使用して、フェールオーバー メカニズムの冗長性を提供していることがわかります。「**管理 | 接続性 | VPN > 基本設定**」に移動します。ファイアウォールで使用される VPN ポリシーの名前は、2 つのポリシーを区別する接尾辞と接続の AWS ID に基づいて決定されます。

2 つの VPN ポリシーで条件が一致すると、2 つのトンネル インターフェースが作成されます。「**管理 | システム セットアップ | ネットワーク > インターフェース**」に移動します。また、VPN 接続の ID に基づく命名規則も使用されます。

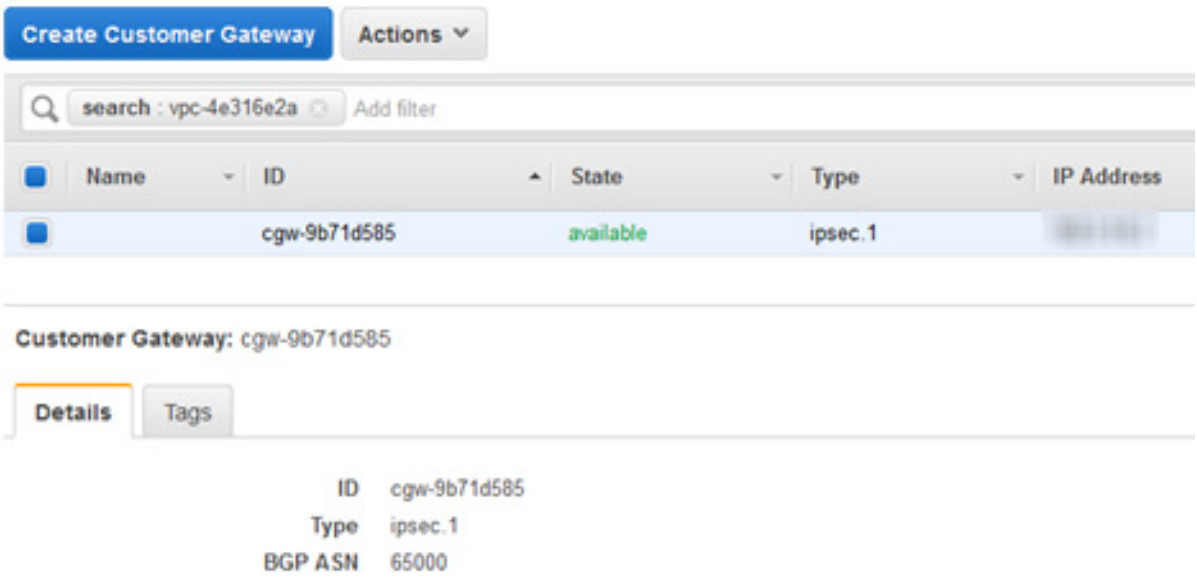
同様に、2 つのルート ポリシーが作成されます。どちらの場合も送信先として VPC を表すアドレス オブジェクトが使用されます。「**管理 | システム セットアップ | ネットワーク > ルーティング**」に移動します。それぞれ異なるトンネル インターフェースが使用されます。

アマゾン ウェブ サービスでの設定

ファイアウォールの GUI にある「AWS VPN」ページから VPN 接続を作成する過程で AWS の設定も変更されます。AWS コンソールを使用して VPC ダッシュボードで VPN 接続を表示します。VPC ID をフィルタとして使用し、作成された VPN 接続を見つけます。



Customer Gateway (カスタマー ゲートウェイ)、ファイアウォールのエンドポイント、最初に VPN 接続を作成したときに指定した IP アドレスは、AWS コンソールでも表示できます。VPC ダッシュボードのカスタマー ゲートウェイ ページに移動します。

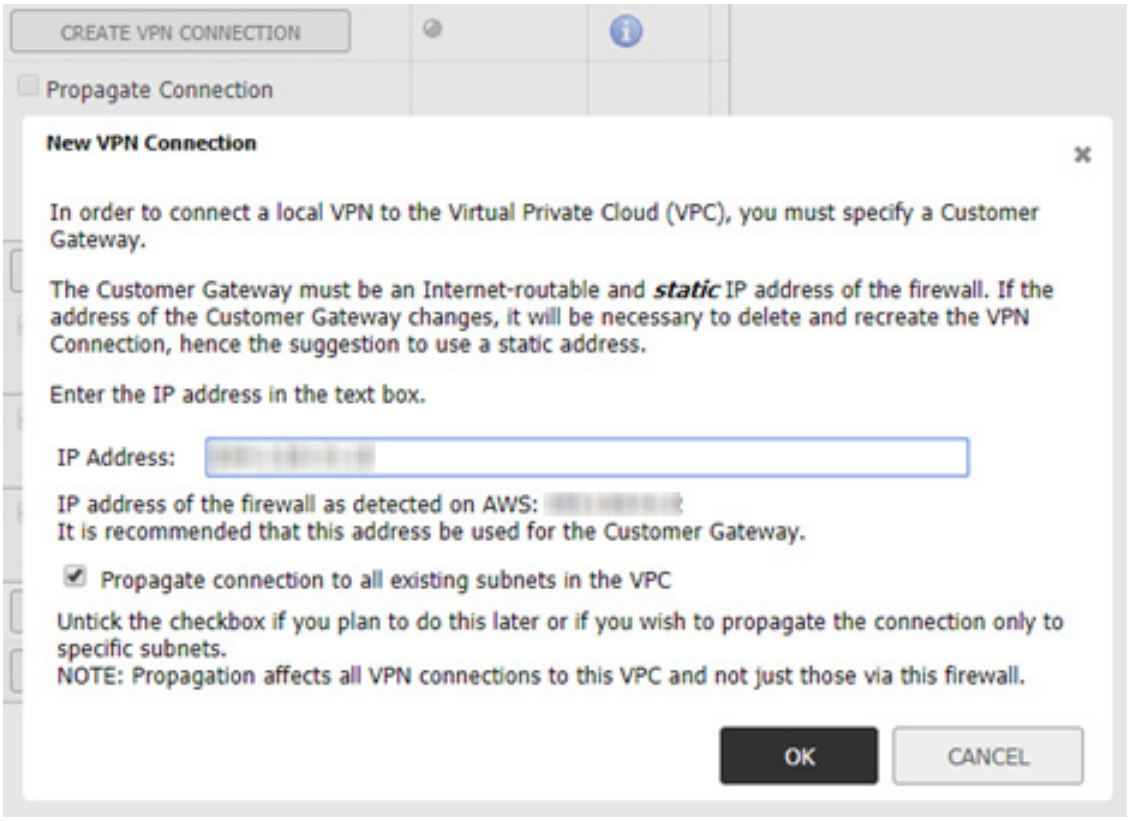


経路伝搬

特定の VPC 内のサブネット上のリソースとの接続を確実に行うために、追加の手順を実行する必要があります。また、関心のあるサブネットで使われているルート テーブルに接続を伝搬する必要があります。3 つの方法を使用して、VPC 内のルート テーブルへの伝搬を有効化できます。

- VPN 接続を作成するとき

  VPC 内の 1 つまたは複数のルート テーブルでルート伝搬が無効になっていることをファイアウォールが検出した場合、ポップアップ ダイアログのチェックボックスを使用して、その VPC 内のすべてのルート テーブルに対してルート伝搬を有効にするよう指定できます。しかし、この方法には一貫性がありません。一部のルート テーブルで伝搬が可能でも、そうでないテーブルがあるからです。

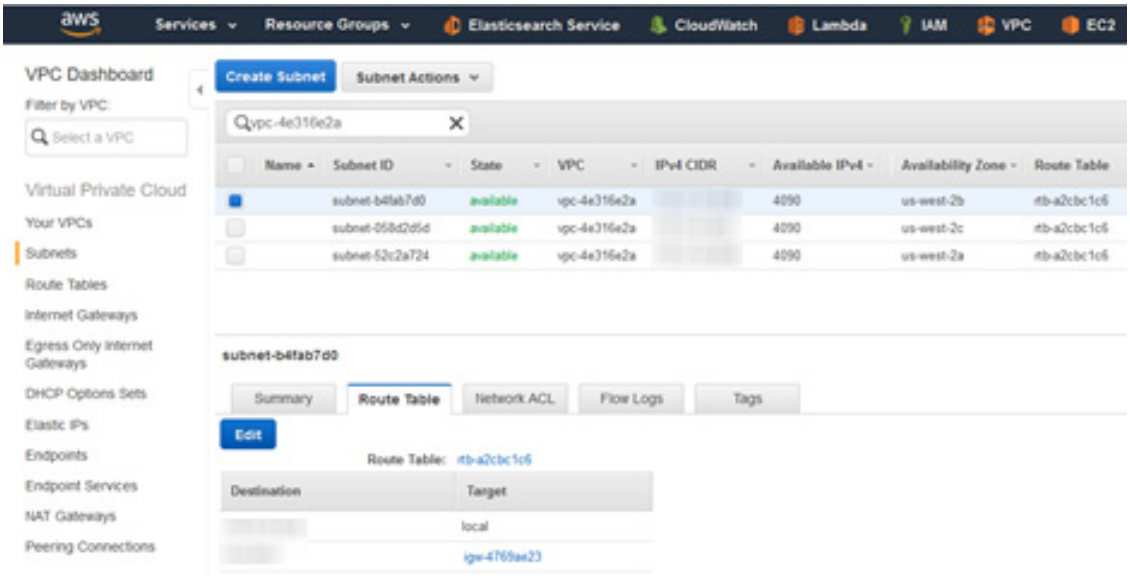


- 各ルート テーブルのチェックボックスの使用

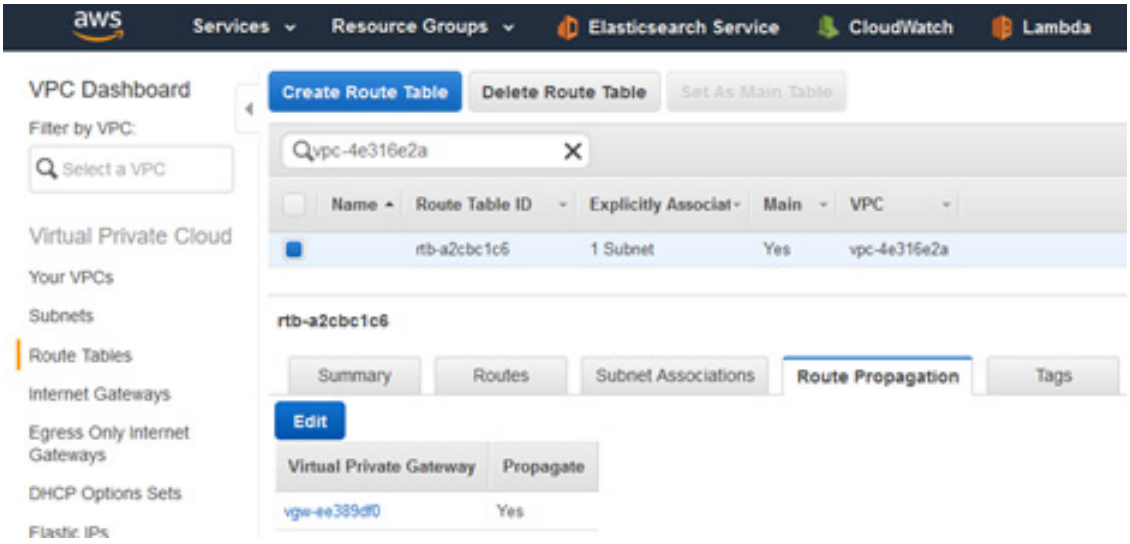
  VPN 接続が確立された後、「AWS VPN」ページ上の VPC テーブルの行を展開すると、その VPC 内のすべてのサブネットがルート テーブルごとに整理されて表示されます。各ルート テーブルの行には、その特定のルート テーブルとそれが管理するサブネットの伝搬を有効または無効にするためのチェックボックスがあります。

- AWS コンソールについて

  各 VPC のサブネットは、AWS コンソール上の VPC ダッシュボードにあるサブネット ページで表示できます。サブネットを選択すると、支配するルート テーブルが特定され、関連するページにジャンプできるようにハイパーリンクが提供されます。



それ以外の場合は、「Route Tables (ルート テーブル)」ページに移動し、フィルタを使用して VPC またはサブネットで検索を絞り込むことができます。



特定のルート テーブルへのルート伝搬を有効または無効にするには:

1 問題のルート テーブルを選択します。

2 「**Route Propagation (ルート伝搬)**」タブを選択します。

3 「**Edit (編集)**」ボタンを選択します。

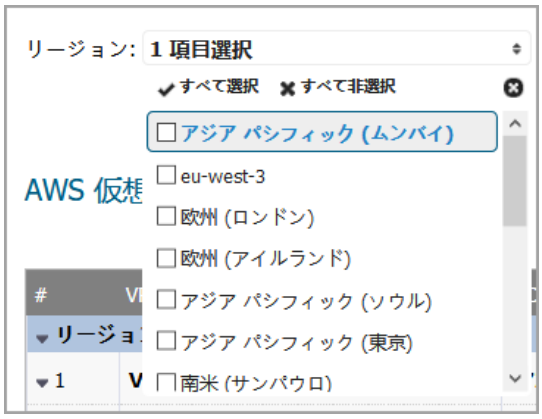
4 必要に応じて、「**Propagate (伝搬)**」チェックボックスをオンまたはオフにします。

5 「**Save (保存)**」ボタンをクリックして変更を確定します。

AWS リージョン

アマゾン ウェブ サービスのリソースは、多数の AWS リージョンに分散しています。顧客は、いずれかまたはすべてのリージョンに VPC を持つことができます。「AWS VPN」ページには、関心のある 1 つまたは複数のリージョンを選択できるドロップダウン コントロールがあります。選択したすべてのリージョンの VPC がテーブルに表示され、それらの VPC のいずれにも新しいVPN 接続を確立できます。

リージョン選択コントロールは、AWS 設定で指定した既定のリージョンで初期化されます。「AWS ログ」ページ上でこれを使用すると、ファイアウォールのログが AWS CloudWatch ログに送信されます。初期の選択とは関係なく、テーブル内の関連する VPC を表示するようにリージョンを選択することもできます。



VPN 接続の削除

「AWS VPN」ページには、不要な VPN 接続を削除する機能があります。

VPC に対応するVPN 接続がある場合、VPC テーブルの関連テーブル行のボタンは、「**VPN 接続の作成**」から「**VPN 接続の削除**」に変更されます。ボタンをクリックすると、システムは確認を求めてから、このファイアウォールまたは他のファイアウォールからの他の VPN 接続に影響を与えずに安全な数の構成設定を削除するプロセスを開始します。これにより、ファイアウォールに設定された、関連する VPN およびルート ポリシーと、トンネル インターフェースが消去されます。AWS では、他で使用されていない場合に限ってカスタマー ゲートウェイが削除されます (別の VPN 接続で同じファイアウォールから他の VPC に接続している場合もあります)。VPN ゲートウェイの削除、またはルート伝搬設定の変更は行われません。


#
VPC/サブネット
CIDR
VPC 状況
VPN 接続の管理
VPN 状況
詳細
リージョン: 米国東部 (バージニア北部) (us-east-1)
1
VPC: vpc-a73c2ddc
available
VPN 接続の削除
available
ルート テーブル: rtb-b6e624c9
サブネット: subnet-cf5c8ca8
available
サブネット: subnet-3a2acb04
available
サブネット: subnet-e7fc2bbb
available
サブネット: subnet-6039a22a
available
サブネット: subnet-5a22f374
available
サブネット: subnet-071a8608
available
VPN の削除
VPN 接続: vpn-003198af352c377cd (仮想プライベート クラウド ID: vpc-a73c2ddc に接続) を削除しますか?
補足: これは、ファイアウォール上の関連付けされた VPN ポリシーを削除します。また、他で使用されていない場合はカスタマー ゲートウェイも削除します。ただし、ルート テーブルに対する伝搬への影響を防ぐために、VPC に関連付けされた仮想プライベート ゲートウェイは削除しません。
はい
いいえ

第 2 部

接続性 | SSL VPN

- SSL VPN について
- SSL VPN サーバの動作の設定
- SSL VPN クライアントの設定
- SSL VPN ウェブポータルの設定
- 仮想オフィスの設定

9

SSL VPN について

このセクションでは、SonicWall ネットワーク セキュリティ装置における SSL VPN 機能の設定方法を説明します。SonicWall の SSN VPN 機能は、NetExtender クライアントを使用してネットワークへのリモート アクセスを保護します。

NetExtender は、Windows、Mac、Linux ユーザ用の SSL VPN クライアントであり、透過的にダウンロードされます。ネットワーク上で任意のアプリケーションを安全に実行でき、ポイント ツー ポイント プロトコル (PPP) を使用できるようになります。NetExtender によって、リモート クライアントはローカル ネットワーク上のリソースにシームレスにアクセスできます。ユーザは、次の 2 通りの方法で NetExtender にアクセスできます。

- SonicWall ネットワーク セキュリティ装置によって提供される仮想オフィス ウェブ ポータルにログインする
- スタンドアロンの NetExtender クライアントを起動する

各 SonicWall 装置は、最大数の現在のリモート ユーザをサポートしています。詳細については、「SSL VPN の最大同時ユーザ数」テーブルを参照してください。

SSL VPN の最大同時ユーザ数

SonicWall 装置モデル	SSL VPN の最大同時接続数	SonicWall 装置モデル	SSL VPN の最大同時接続数	SonicWall 装置モデル	SSL VPN の最大同時接続数
NS*a* 9650	3000	SM 9600	3000	TZ600/TZ600P	200
NS*a* 9450	3000	SM 9400	3000		
NS*a* 9250	3000	SM 9200	3000	TZ500/TZ500 W	150
NS*a* 6650	1500	NSA 6600	1500	TZ400/TZ400 W	100
NS*a* 5650	1500	NSA 5600	1000	TZ300/TZ300 W / TZ300P	50
NS*a* 4650	1000	NSA 4600	500		
NS*a* 3650	500	NSA 3600	350	SOHO W	50
NS*a* 2650	350	NSA 2600	250		

SonicOS は IPv6 アドレスによるユーザ向けの NetExtender 接続をサポートしています。アドレス オブジェクトのドロップダウン リストには、すべての IPv6 アドレス オブジェクトが含まれています。

メモ：IPv6 Wins サーバは *サポートされていません*。IPv6 FQDN がサポートされています。

メモ：SonicOS 6.5.3 以降では、「**管理 | システム設定 | 装置 > 基本設定**」ページの「**無線制御モード**」が「**フル機能ゲートウェイ**」または「**無線なし**」に設定されているとき、**SSL VPN** 接続性を利用できます。「**無線制御モード**」で「**無線制御のみ**」が有効になっている場合、**SSL VPN** インターフェースは使用 ***できず***、「**SSL VPN > サーバ設定 > ゾーン上の SSL VPN 状況**」の状況表示はすべてのゾーンで停止中となり、**SSL VPN** ゾーンは編集できません。詳細については、『*SonicOS 6.5 システム設定* 管理ガイド』を参照してください。

トピック:

- NetExtender について
- SSL VPN アクセスのためのユーザの設定
- 生体認証

NetExtender について

SonicWall の SSL VPN NetExtender は、Windows、Mac、Linux ユーザがリモート ネットワーク向けの透過的なソフトウェア アプリケーションであり、その機能を使うことでユーザは会社のネットワークにセキュアな方法で接続できます。NetExtender により、リモート ユーザは会社のネットワーク上の任意のアプリケーションを安全に実行できます。ファイルのアップロード/ダウンロード、ネットワーク ドライブのマウント、リソースへのアクセスといった作業がローカル ネットワークにいる感覚で行えます。

NetExtender により、リモート ユーザは保護された内部ネットワークへのフル アクセスが可能になります。その体験は従来の IPsec VPN クライアントの使用体験とほぼ同じですが、Windows 用の NetExtender クライアントは、Firefox の使用時には XPCOM プラグインを使用しているリモート ユーザの PC に自動的にインストールされます。MacOS システムの場合は、サポート対象のブラウザが Java コントロールを使用して、仮想オフィス ポータルから NetExtender を自動的にインストールしてくれます。Linux システムでも、NetExtender クライアントをインストールして使用することができます。Windows ユーザは、ポータルからクライアントをダウンロードする必要があり、モバイル機器を使用している Windows ユーザは、アプリ ストアから Mobile Connect をダウンロードする必要があります。

NetExtender スタンドアロン クライアントは、ユーザによる NetExtender の初回起動時にインストールできます。そのため、Windows システムでは「**スタート**」メニューから、MacOS システムでは**アプリケーション** フォルダまたはドックからの直接アクセスが可能です。また Linux システムでも、パス名によって、あるいはショートカット バーから直接アクセスできます。

インストール後、NetExtender が自動的に起動し、SSL VPN を利用した安全なポイントツーポイント アクセスによって内部ネットワーク上の許可されたホストおよびサブネットにアクセスするための仮想アダプタに接続します。

トピック:

- NetExtender 範囲に対するアドレス オブジェクトの作成
- アクセスの設定
- プロキシの設定
- スタンドアロン クライアントのインストール

NetExtender 範囲に対するアドレス オブジェクトの作成

NetExtender 設定の一部として、NetExtender IP アドレス範囲に対するアドレス オブジェクトを作成する必要があります。その後、このアドレス オブジェクトはデバイス プロファイルの設定時に使用します。

使用する IPv4 アドレス範囲と IPv6 アドレス範囲の両方のアドレス オブジェクトを、「**SSL VPN > クライアント設定**」で作成できます。アドレス オブジェクトで設定されるアドレス範囲は、NetExtender セッション中にリモート ユーザに割り当てられるアドレスを含む IP アドレス プールを定義します。この範囲は、サポートする NetExtender 同時ユーザの最大数に対応できる大きさにする必要があります。さらにアドレスを追加して対応数を増やすことはできますが、これは必須ではありません。

メモ：装置と同じセグメント上に他のホストが存在する場合は、アドレス範囲が、他の割り当て済みアドレスと重複したり衝突したりしないようにしてください。

アドレス オブジェクトの詳しい設定方法は、「**アドレス オブジェクト**」セクションの「*SonicOS 6.5 ポリシー*」に記載されています。SSL アドレス オブジェクトの定義に必要な設定については、クイック リファレンスを参照してください。

NetExtender IP アドレス範囲に対するアドレス オブジェクトを作成するには:

1. 「**管理 | ポリシー | オブジェクト > アドレス オブジェクト**」に移動します。
2. 「**追加**」を選択します。
3. 「**名前**」フィールドにわかりやすい名前を入力します。
4. 「**ゾーンの割り当て**」で、「**SSLVPN**」を選択します。
5. 「**種別**」で、「**範囲**」を選択します。
6. 「**開始アドレス**」フィールドに、使用するアドレス範囲内の最小 IP アドレスを入力します。

   メモ：IP アドレス範囲は、SSL VPN サービスで使用されるインターフェースと同じサブネット上になければなりません。
7. 「**終了アドレス**」フィールドに、使用するアドレス範囲内の最大 IP アドレスを入力します。
8. 「**追加**」を選択します。
9. 「**閉じる**」を選択します。

アクセスの設定

NetExtender クライアント ルートは、SSL VPN ユーザによる各種ネットワーク リソースへのアクセスを許可または拒否するために使用されます。アドレス オブジェクトを使用することで、ネットワーク リソースへのアクセスを動的かつ容易に設定できます。 **強制トンネル**方式では、リモート ユーザとやり取りされるすべてのトラフィックが (リモート ユーザのローカル ネットワークへのトラフィックを含め) SSL VPN NetExtender トンネルを経由します。これは、次のルートをリモート クライアントのルート テーブルに追加することで実行されます。

リモート クライアントのルート テーブルに追加されるルート

IP アドレス	サブネット マスク
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender は、接続中のすべてのネットワーク接続のローカル ネットワーク ルートも追加します。これらのルートには既存のルートよりも高いメトリックが設定されているため、ローカル ネットワークへのトラフィックは強制的に SSL VPN トンネル経由に切り替えられます。例えば、リモート ユーザが

10.0.*.* ネットワークの IP アドレス 10.0.67.64 を使用している場合、ルート 10.0.0.0/255.255.0.0 が追加され、トラフィックが SSL VPN トンネルを経由するようになります。

メモ：強制トンネル方式を設定するにはまた、0.0.0.0 のアドレス オブジェクトを設定して、SSL VPN NetExtender ユーザとグループがこのアドレス オブジェクトへのアクセスを持つように割り当てる必要があります。

管理者も、NetExtender の接続が確立されたときにバッチ ファイル スクリプトを実行できます。これらのスクリプトを使って、ネットワーク ドライブやプリンタのマッピングおよび切断、アプリケーションの起動、ファイルやウェブ サイトの表示などを行うことができます。NetExtender の接続スクリプトでは任意の有効なバッチ ファイル コマンドを使用できます。

プロキシの設定

SonicWall SSL VPN は、プロキシ設定を使用した NetExtender セッションをサポートしています。現在サポートされているのは、HTTPS プロキシのみです。NetExtender をウェブ ポータルから起動する場合、プロキシ アクセスを行うようにブラウザが既に設定されているときは、NetExtender が自動的にそのプロキシ設定を継承します。プロキシ設定は、NetExtender クライアントでの手動設定も可能です。NetExtender は、Web Proxy Auto Discovery (WPAD) プロトコルに対応したプロキシ サーバ用のプロキシ設定を自動的に検出できます。

NetExtender には、次の 3 つのプロキシ設定オプションが用意されています。

- 「**設定を自動検出する**」- この設定を使用するには、プロキシ サーバが Web Proxy Auto Discovery Protocol プロトコルをサポートしていて、プロキシ設定スクリプトをクライアントに自動送信できる必要があります。
- **自動設定スクリプトを使用する** - プロキシ設定スクリプトの場所がわかっている場合は、このオプションを選択してスクリプトの URL を指定することができます。
- **プロキシ サーバを使用する** - このオプションを選択すると、プロキシ サーバの IP アドレスとポートを指定できます。また、「**プロキシのバイパス**」フィールドに IP アドレスまたはドメインを入力すれば、それらのアドレスに直接接続してプロキシ サーバをバイパスすることができます。必要に応じて、プロキシ サーバ用のユーザ名とパスワードも入力できます。プロキシ サーバがユーザ名とパスワードを要求しているのにそれらを指定していない場合は、最初の接続時に NetExtender のポップアップ ウィンドウが表示され、その入力を求められます。

プロキシ設定を使用して接続する場合、NetExtender は、ファイアウォールのサーバに直接接続せず、プロキシ サーバへの HTTPS 接続を確立します。その後、プロキシ サーバによってトラフィックが SSL VPN サーバに転送されます。すべてのトラフィックは、NetExtender とネゴシエートされた証明書を使って SSL によって暗号化されます。 これについては、プロキシ サーバ側は関知していません。プロキシを使用してもしなくても、接続のプロセスに違いはありません。

スタンドアロン クライアントのインストール

NetExtender スタンドアロン クライアントは、NetExtender の初回起動時にユーザの PC または Mac に自動的にインストールされます。あるいは、インストーラをダウンロードしてユーザのシステムで実行することもできます。インストーラでは、ユーザのログイン情報に基づいてプロファイルが作成されます。その後、インストーラのウィンドウが閉じ、NetExtender が自動的に起動します。旧バージョンの NetExtender が既にインストールされていた場合、インストーラは古い NetExtender を最初にアンインストールするかユーザにアンインストールするよう要求し、その後、新バージョンをインストールできます。

NetExtender スタンドアロン クライアントのインストール後、Windows の場合は「**スタート > プログラム**」メニューまたはシステム トレーを使用して NetExtender を起動し、Windows の起動時に NetExtender が起動されるように設定できます。Mac の場合は、システムの**アプリケーション** フォルダから NetExtender を起動できます。また、アイコンをドックにドラッグしてすばやくアクセスすることもできます。Linux システムでは、インストーラによってデスクトップ ショートカットが **/usr/share/NetExtender** に作成されます。このショートカットは、Gnome や KDE といった環境のショートカット バーにドラッグできます。

メモ： SonicWall 装置に NetExtender をインストールする詳細は手順については、ナレッジ ベースの記事「SonicOS 5.9 以降で SSL-VPN 機能 (NetExtender アクセス) を設定する方法 (SW10657)」を参照してください。

ビデオ：「How to configure SSL VPN」(SSL VPN の設定方法) というビデオでも NetExtender の設定手順を説明しています。

SSL VPN アクセスのためのユーザの設定

ユーザは、SSL VPN サービスにアクセスできるためには、**SSLVPN サービス** グループに割り当てられている必要があります。「**SSLVPN サービス**」グループに属していないユーザが仮想オフィスからログインを試みても、アクセスは拒否されます。

トピック:

- ローカル ユーザの場合
- RADIUS および LDAP ユーザの場合
- 強制トンネル方式アクセスの場合

ローカル ユーザの場合

ローカル ユーザおよびグループの詳しい追加方法と設定方法が、「**ユーザ**」セクションの「*SonicOS 6.5 システム設定*」に記載されています。以下はクイック リファレンスで、SSLVPN サービスの有効化に必要なユーザ設定が記載されています。

ローカル ユーザ向けの SSL VPN アクセスを設定するには、以下の手順に従います。

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. 設定したいユーザに対する**編集**アイコンを選択するか、「**ユーザの追加**」ボタンを選択して新しいユーザを作成します。
3. 「**グループ**」を選択します。
4. 「**ユーザ グループ**」列の「**SSLVPN サービス**」を選択し、「**右矢印**」を選択してこれを「**所属するグループ**」列に移動します。

5 「**VPN アクセス**」を選択し、適切なネットワーク リソース VPN ユーザ (GVC、NetExtender、または仮想オフィス ブックマーク) を「**アクセス リスト**」に移動します。

> **メモ：**「**VPN アクセス**」設定は、GVC、NetExtender、または SSL VPN 仮想オフィス ブックマークを使ってネットワーク リソースにアクセスするリモート クライアントの能力に影響します。GVC、NetExtender、または仮想オフィスのユーザにネットワーク リソースへのアクセスを許可するには、ネットワーク アドレス オブジェクトかグループを「**VPN アクセス**」の「**アクセス リスト**」に追加する必要があります。

6 「**OK**」を選択します。

RADIUS および LDAP ユーザの場合

RADIUS ユーザと LDAP ユーザの設定手順は同様です。これらのユーザを「SSLVPN サービス」ユーザ グループに追加する必要があります。

ユーザ グループの詳しい追加方法と設定方法が、「**ユーザ**」セクションの「*SonicOS 6.5 システム設定*」に記載されています。以下はクイック リファレンスで、ユーザを適切なグループに追加するために必要なユーザ設定が記載されています。

RADIUS ユーザおよび LDAP ユーザ向けの SSL VPN アクセスを設定するには、以下の手順に従います。

共通ステップ	RADIUS ユーザの設定	LDAP ユーザの設定
1 「**管理**」表示を選択します。		
2 「**ユーザ > 設定**」に移動します。		
3 「**認証**」を選択します。		
4 「**ユーザ認証方式**」フィールドで：	「**RADIUS**」または「**RADIUS + ローカル ユーザ**」を選択します。	「**LDAP**」または「**LDAP + ローカル ユーザ**」を選択します。
5 選択：	**RADIUS の設定**	**LDAP の設定**
6 選択：	**RADIUS ユーザ**	**ユーザとグループ**
7 適切なフィールドの「**SSLVPN サービス**」を選択します。	**すべての RADIUS ユーザが初期状態で所属するグループ**	**既定の LDAP ユーザ グループ**
8 「OK」を選択します。		

強制トンネル方式アクセスの場合

ローカル ユーザおよびグループの詳しい追加方法と設定方法が、「**ユーザ**」セクションの「*SonicOS 6.5 システム設定*」に記載されています。以下はクイック リファレンスで、「**強制トンネル**」方式に対してユーザとグループを設定するために必要なユーザ設定が記載されています。

SSL VPN NetExtender ユーザとグループを強制トンネル方式のために設定するには、以下の手順を実行します。

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 SSL VPN NetExtender ユーザまたはグループに対する「**設定**」アイコンを選択します。

3 「**VPN アクセス**」を選択します。

4 「**WAN リモート アクセス ネットワーク**」アドレス オブジェクトを選択し、**右矢印**ボタンをクリックして「**アクセス リスト**」まで移動させます。

5 「**OK**」を選択します。

6 SSL VPN NetExtender を使うすべてのローカル ユーザおよびグループに対して、このプロセスを繰り返します。

生体認証

重要：生体認証を使用するには、モバイル デバイスに Mobile Connect 4.0 以上をインストールしてファイアウォールに接続しておく必要があります。

SonicOS は、SonicWall Mobile Connect と連携して生体認証をサポートしています。Mobile Connect は、ユーザがモバイル デバイスからプライベート ネットワークに安全にアクセスできるようにするアプリです。Mobile Connect 4.0 では、ユーザ名とパスワードの代わりにフィンガー タッチによる認証を使用できます。

この認証方法を許可する設定項目は「**SSL VPN > クライアント設定**」ページにあります。これらのオプションが表示されるのは、「モバイル接続」を使用してファイアウォールに接続している場合のみとなります。

「**SSL VPN > クライアント設定**」ページで生体認証を設定した後、ユーザのスマートフォンまたはその他のデバイスで、TouchID (iOS) または指紋認証 (Android) を有効にする必要があります。

10

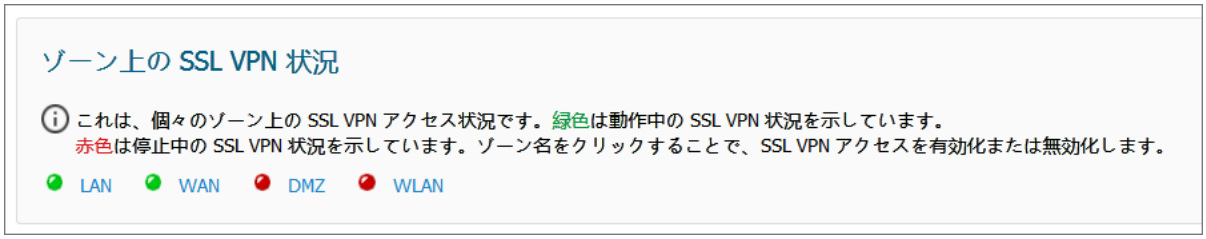
SSL VPN サーバの動作の設定

「**SSL VPN > サーバ設定**」ページでは、SSL VPN サーバとして機能するファイアウォールを設定します。

トピック:

- ゾーン上の SSL VPN 状況
- SSL VPN サーバ設定
- RADIUS ユーザの設定
- SSL VPN クライアント ダウンロード URL

ゾーン上の SSL VPN 状況



このセクションには、ゾーンごとの SSL VPN アクセス状況が表示されます。

- 緑色は、SSL VPN が有効であることを示します。
- 赤色は、SSL VPN が無効であることを示します。

SSL VPN アクセスを有効または無効にするには、ゾーン名を選択します。

SSL VPN サーバ設定

SSL VPN サーバを設定するには:

1 **SSL VPN ポート** - SSL VPN ポート番号を入力します。既定値は **4433** です。

2 **証明書の選択**: SSL VPN ユーザを認証するために使う証明書を、ドロップダウン メニューから選択します。既定の方法は、「**自己署名証明書を使用**」です。

3 **ユーザ ドメイン** - ユーザのドメインを入力します。これは、NetExtender クライアントのドメイン フィールドと一致する必要があります。既定は「**LocalDomain**」です。

> **メモ**：認証パーティションを使用していない場合、このフィールドの値は、NetExtender クライアントのドメイン フィールドと一致している必要があります。
>
> 認証パーティションを使用している場合は、NetExtender で、そのパーティションを使用して設定されたドメイン名のいずれかをユーザが入力できるため、RADIUS または LDAP 経由で外部から名前/パスワードの認証を行う場合にこのパーティションを選択します。この場合、ここで設定される名前はユーザがローカル認証のために入力する既定の名前 (またはローカル アカウントを持っていないユーザが既定のパーティションで認証のために入力する既定の名前) となります。
>
> いずれの場合も、このユーザのドメイン名は、外部認証を取得して使用すると RADIUS/LDAP サーバには送信されず、外部認証がない単純なユーザ名が送信されます。

4 **SSL VPN でウェブ管理を有効にする** - SSL VPN を介したウェブ管理を有効にするには、このドロップダウン メニューから「**有効**」を選択します。既定は「**無効**」です。

5 **SSL VPN で SSH 管理を有効にする** - SSL VPN を介した SSH 管理を有効にするには、このドロップダウン メニューから「**有効**」を選択します。既定は「**無効**」です。

6 **無動作時タイムアウト (分)** - ユーザをログアウトさせるまでの無動作時間を分単位で入力します。既定値は **10** 分です。

7 ページ下部にある「**適用**」を選択します。

RADIUS ユーザの設定

このセクションは、「**管理 | システム セットアップ | ユーザ > 設定**」ページで SSL VPN ユーザを認証するために RADIUS と LDAP のどちらかを設定したときだけ使用できます。RADIUS の MSCHAP モードが有効になっている場合、ユーザはログイン時に期限切れのパスワードを変更できます。

MSCHAP または MSCHAPv2 モードを設定するには:

1 「**RADIUS を以下のモードで使用する**」チェックボックスをオンにします。

2 次の 2 つのモードのどちらかを選択します。

- **MSCHAP**
- **MSCHAPV2**

> **メモ**：LDAP では、Active Directory (アクティブ ディレクトリ) を TLS と共に使用して管理アカウントでそれにバインドしている場合か Novell eDirectory (ノベル イーディレクトリ) を使用している場合にのみ、パスワードを変更できます。
>
> このオプションが設定されており、「**ユーザ > 設定**」ページの「ログインの認証方法」として LDAP が選択されているが、LDAP がパスワードの更新を許可する設定になっていない場合、LDAP を使用してユーザ認証が行われた後で、MSCHAP モードの RADIUS を使用して SSL VPN クライアント ユーザのパスワードの更新が実行されます。

3 ページ下部にある「**適用**」を選択します。

SSL VPN クライアント ダウンロード URL

このページのこのセクションでは、クライアント システムによる SSL VPN クライアントのダウンロード元を設定します。装置からファイルをダウンロードしてウェブ サーバに配置することで、このクライアント パッケージをホストする独自のサーバを提供できます。それ以外の場合、クライアントはファイアウォールから SSL VPN ファイルをダウンロードできます。

SSL VPN クライアント ファイルのダウンロード用に独自のウェブ サーバを設定するには:

1 「**ここを選択すると、すべての SSL VPN クライアント ファイルが含まれた SSL VPN zip ファイルをダウンロードします**」のリンクを選択して、すべてのクライアント SSL VPN ファイルを装置からダウンロードします。ファイルを開いて解凍し、HTTP サーバ上のフォルダに置きます。

2 「**顧客の HTTP サーバをダウンロード URL として使用する: (http://)**」チェックボックスをオンにして、表示されたフィールドに SSL VPN クライアント ダウンロード URL を入力します。

3 「**適用**」を選択します。

11

SSL VPN クライアントの設定

「**SSL VPN > クライアント設定**」ページで、既定のデバイス プロファイルと SonicPoint/SonicWave L3 管理の既定のデバイス プロファイルを編集できます。既定のデバイス プロファイルは、ゾーン上の SSL VPN アクセスの有効化を可能にして、クライアント ルートの設定、クライアント DNS と NetExtender の設定を行います。SonicPoint/SonicWave L3 管理の既定のデバイス プロファイルには、SSL VPN アクセス、クライアント ルート、および SonicPoint/SonicWave 無線アクセス ポイント経由で接続するクライアントのレイヤ 3 設定を構成するための設定が含まれています。

「**SSL VPN > クライアント設定**」ページには、SSL VPN アクセスが有効化されている設定済みの IPv4 および IPv6 ネットワーク アドレスとゾーンも表示されます。

トピック:

- 既定のデバイス プロファイルの設定
- IPv6 用のデバイス プロファイルの設定
- SonicPoint/SonicWave L3 管理の既定のデバイス プロファイルの設定

既定のデバイス プロファイルの設定

既定のデバイス プロファイルを編集して、ゾーンと NetExtender アドレス オブジェクトを選択し、クライアント ルートを設定し、クライアント DNS と NetExtender を設定します。

SSL VPN アクセスがゾーン上で有効になっていなければ、ユーザは仮想オフィス ウェブ ポータルにアクセスできません。SSL VPN アクセスは、「**管理 | システム セットアップ | ネットワーク > ゾーン**」ページで設定できます。詳細については、ネットワーク セクションの *SonicOS 6.5 システム設定* 管理ドキュメントを参照してください。

トピック:

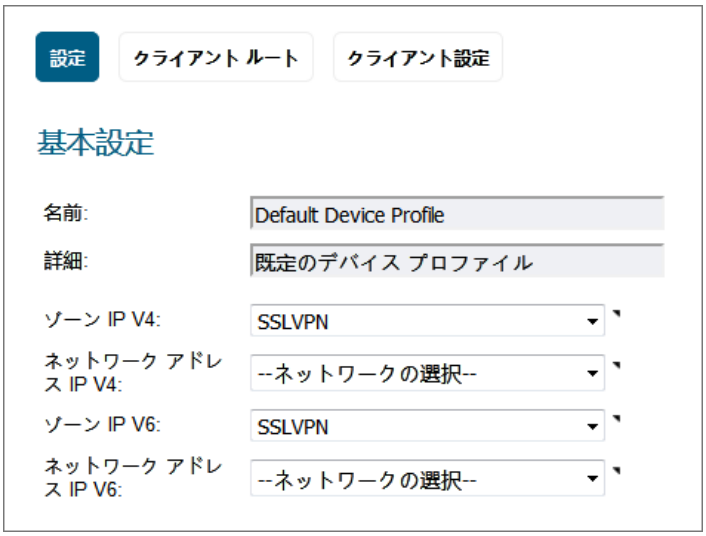
- 設定オプションの設定
- クライアント ルートの設定
- クライアント設定の指定

設定オプションの設定

既定のデバイス プロファイルの設定オプションの設定を行うには

1 「**管理 | 接続性 | SSL VPN > クライアント設定**」ページに移動します。

2 「**既定のデバイス プロファイル**」の**編集**アイコンをクリックします。



メモ：「**既定のデバイス プロファイル**」の「**名前**」と「**詳細**」は変更できません。

3 このプロファイルのゾーン バインド設定を行うには、「**ゾーン IP V4**」ドロップダウン メニューから「**SSL VPN**」またはユーザ定義のゾーンを選択します。

4 「**ネットワーク アドレス IP V4**」ドロップダウン メニューで、このプロファイル用に作成済みの IPv4 NetExtender アドレス オブジェクトを選択します。詳細については、「NetExtender 範囲に対するアドレス オブジェクトの作成」を参照してください。この設定により、このプロファイルの IP プールとゾーン バインド設定が選択されます。NetExtender クライアントは、このプロファイルと一致する場合、このアドレス オブジェクトから IP アドレスを取得します。

5 このプロファイルのゾーン バインド設定を行うには、「**ゾーン IP V6**」ドロップダウン メニューから **SSLVPN** またはユーザ定義のゾーンを選択します。

6 「**ネットワーク アドレス IP V6**」ドロップダウン メニューで、作成済みの IPv6 NetExtender アドレス オブジェクトを選択します。

7 「**OK**」を選択して、設定を保存し、ウィンドウを閉じます。または、「クライアント ルートの設定 (137 ページ)」に進みます。

クライアント ルートの設定

「**クライアント ルート**」では、SSL VPN ユーザに許可するネットワーク アクセスを制御できます。NetExtender クライアント ルートは、すべての NetExtender クライアントに渡され、SSL VPN 接続経由でリモート ユーザがアクセスできるプライベート ネットワークおよびリソースの決定に使用されます。

クライアント ルートの設定を行うには、以下の手順に従います。

1 「**管理 | 接続性 | SSL VPN > クライアント設定**」ページに移動します。

2 「**既定のデバイス プロファイル**」の**編集**アイコンをクリックします。

3 「**クライアント ルート**」を選択します。

4 NetExtender ユーザに対するすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) を強制的に SSL VPN NetExtender トンネルに通すには、「**強制トンネル方式**」ドロップダウン リストから「**有効**」を選択します。

5 「**ネットワーク**」で、SSL VPN アクセスを許可するアドレス オブジェクトを選択します。

6 **右矢印**ボタンを選択して、選択したアドレス オブジェクトを「**クライアント ルート**」リストに移します。

7 クライアント ルートに使用するすべてのアドレス オブジェクトを移し終えるまで繰り返します。

クライアント ルートを作成すると、アクセス ルールも自動的に作成されます。SSL VPN ゾーンに対するアクセス ルールを手動で設定することもできます。アクセスルールの設定方法の詳細については、*SonicOS 6.5 ポリシー*を参照してください。

8 「**OK**」を選択して、設定を保存し、ウィンドウを閉じます。または、「クライアント設定の指定 (138 ページ)」に進みます。

クライアント設定の指定

「クライアント設定」画面には、オプションを含む次の 2 つのセクションがあります。

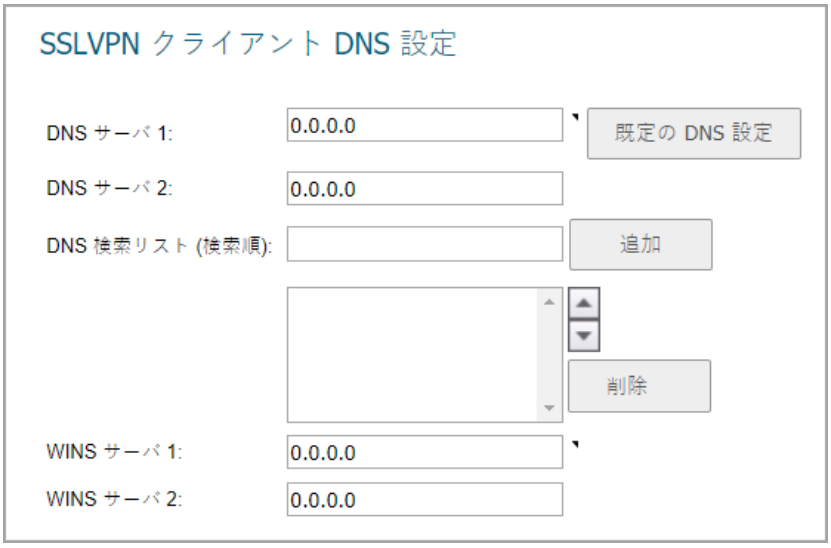
- SSLVPN クライアント DNS 設定
- NetExtender クライアントの設定

SSLVPN クライアント DNS 設定を行うには、以下の手順に従います。

1 「**管理 | 接続性 | SSL VPN > クライアント設定**」ページに移動します。

2 「**既定のデバイス プロファイル**」の**編集**アイコンをクリックします。

3 「**クライアント設定**」を選択します。画面上部に、「**SSLVPN クライアント DNS 設定**」セクションが表示されます。



4 「**DNS サーバ 1**」フィールドで、次のいずれかを行います。

- プライマリ DNS サーバの IP アドレスを入力します。
- 「**既定の DNS 設定**」をクリックして、「**DNS サーバ 1**」と「**DNS サーバ 2**」の両方のフィールドで既定の設定を使用します。フィールドは自動的に設定されます。

メモ：IPv4 と IPv6 の両方がサポートされています。

5 (オプション)「**既定の DNS 設定**」を選択しなかった場合は、「**DNS サーバ 2**」フィールドにバックアップ DNS サーバの IP アドレスを入力します。

6 (オプション) **DNS 検索リスト**を構築するには以下の手順に従います。

a 「**DNS 検索リスト (検索順)**」フィールドに、DNSサーバの IP アドレスを入力します。

b 「**追加**」を選択して、下のリストにそれを追加します。

c 必要なだけ を繰り返します。

リストの順序を変更するには、アドレスの 1 つを選択し、上下の矢印ボタンを使用してその位置を変更します。リストからアドレスを削除するには、アドレスを選択して「**削除**」を選択します。

7 (オプション)「**WINS サーバ 1**」フィールドに、プライマリ WINS サーバの IP アドレスを入力します。

メモ：IPv4 のみがサポートされています。

8 (オプション)「**WINS サーバ 2**」フィールドに、バックアップ WINS サーバの IP アドレスを入力します。

9 スクロールして「**NetExtender クライアント設定**」を指定して、ユーザの接続および切断時の NetExtender の動作をカスタマイズします。

10 次の各設定に対して「**有効**」または「**無効**」を選択します。既定では、すべてが「**無効**」に設定されています。

NetExtender クライアントの設定	定義
クライアントの自動更新を有効にする	NetExtender クライアントを起動するたびにアップデートの有無をチェックします。
切断後にクライアントを終了	SSL VPN サーバから切断されると、NetExtender クライアントは終了されます。再接続するには、ユーザは SSL VPN ポータルに戻るか、ローカル システムで NetExtender クライアントを起動する必要があります。
iOS 機器のタッチ ID を許可する	NetExtender クライアントにより、iOS スマートフォンでのタッチ ID 認証が可能になります。
Android 機器の指紋認証を許可する	NetExtender クライアントにより、Android 機器での指紋認証が可能になります。
NetBIOS over SSL VPN を有効にする	NetExtender クライアントにより、NetBIOS プロトコルが使用可能になります。
クライアント終了後にアンインストール	SSL VPN サーバから切断された NetExtender クライアントはアンインストールされます。再接続するには、SSL VPN ポータルに戻る必要があります。
クライアント接続プロファイルを作成	NetExtender クライアントは、SSL VPN サーバの名前、ドメイン名、およびユーザ名とパスワード (これはオプション) が記録された接続プロファイルを作成します。

11 ユーザが NetExtender クライアントにユーザ名とパスワードをキャッシュできるようにするかどうかを設定するには、「**ユーザ名とパスワードの保存**」フィールドで次のいずれかの動作を選択します。これらのオプションによって、セキュリティの必要性とユーザの使い勝手のバランスに配慮した設定を行うことができます。

- **ユーザ名だけ保存を許可**
- **ユーザ名とパスワードの保存を許可**
- **ユーザ名とパスワードの保存を禁止**

12 「**OK**」を選択します。

IPv6 用のデバイス プロファイルの設定

SonicOS は IPv6 アドレスによるユーザ向けの NetExtender 接続をサポートしています。「**SSL VPN > クライアント設定**」ページで、まず従来の IPv4 IP アドレス プールを設定し、次に IPv6 IP プールを設定します。クライアントには、IPv4 と IPv6 の 2 つの内部アドレスが割り当てられます。

メモ：IPv6 Wins サーバはサポートされていません。

「**SSL VPN > クライアント ルート**」ページで、事前定義されたすべての IPv6 アドレス オブジェクトを含むすべてのアドレス オブジェクトのドロップダウン リストからクライアント ルートを選択できます。

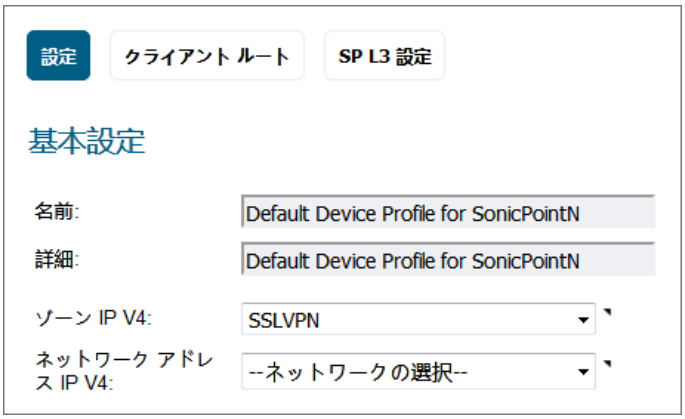
メモ：IPv6 FQDN がサポートされています。

SonicPoint/SonicWave L3 管理の既定のデバイス プロファイルの設定

このセクションでは、SSL VPN アクセス、クライアント ルート、および SonicPoint/SonicWave 無線アクセス ポイント経由で接続するクライアントのレイヤ 3 設定を構成する方法について説明します。

SonicPoint L3 プロファイルを設定するには:

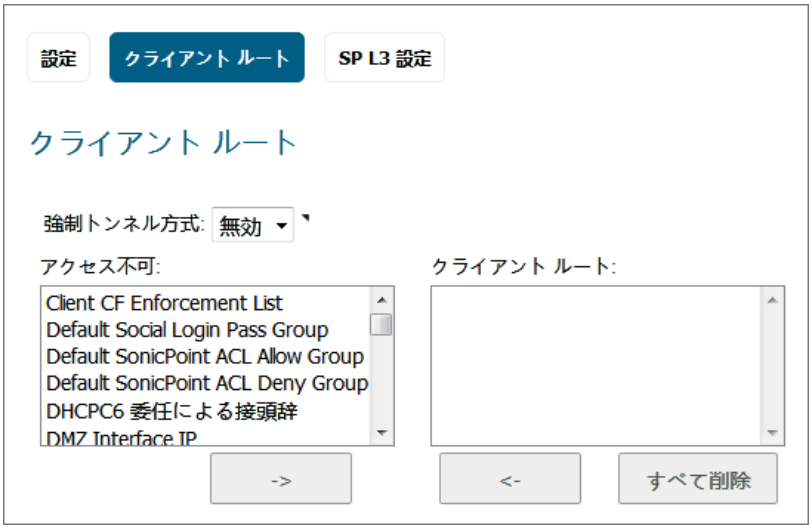
1. 「**管理 | 接続性 | SSL VPN > クライアント設定**」ページに移動します。
2. 「**SonicPoint/SonicWave L3 管理の既定のデバイス プロファイル**」で、**SonicPointN の既定のデバイス プロファイル**の「**編集**」アイコンを選択します。



メモ：「**名前**」と「**説明**」は、変更できません。

3. 「**設定**」画面で、「**ゾーン IP V4**」ドロップダウン リストから **SSLVPN** またはユーザ定義ゾーンを選択して、このプロファイルのゾーン バインド設定を行います。
4. 「**ネットワーク アドレス IP V4**」ドロップダウン メニューで、作成済みの IPv4 NetExtender アドレス オブジェクトを選択するか、「**ネットワークの作成**」を選択してネットワークを作成します。詳細については、「NetExtender 範囲に対するアドレス オブジェクトの作成 (127 ページ)」を参照してください。この設定により、このプロファイルの IP プールとゾーン バインド設定が選択されます。NetExtender クライアントは、このプロファイルと一致する場合、このアドレス オブジェクトから IP アドレスを取得します。

5 「**クライアント ルート**」を選択します。



6 NetExtender ユーザに対するすべてのトラフィック (リモート ユーザのローカル ネットワーク宛てのトラフィックも含む) を強制的に SSL VPN NetExtender トンネルに通すには、「**強制トンネル方式**」ドロップダウン リストから「**有効**」を選択します。

7 「**アクセス不可**」リストから、SSL VPN アクセスを許可するアドレス オブジェクトを選択します。

8 **右矢印**を選択して、選択したアドレス オブジェクトを「**クライアント ルート**」リストに移します。

9 クライアント ルートに使用するすべてのアドレス オブジェクトを移し終えるまで繰り返します。

クライアント ルートを作成すると、このアクセスを許可するアクセス ルールが自動的に作成されます。あるいは、「**管理 | ポリシー | ルール > アクセス ルール**」ページで、SSL VPN ゾーンに対するアクセス ルールを手動で設定することもできます。アクセスルールの設定方法の詳細については、*SonicOS 6.5 ポリシー*を参照してください。

メモ：SSL VPN のクライアント ルートを設定した後で、すべての SSL VPN NetExtender ユーザとユーザグループがクライアント ルートにアクセスできるよう設定する必要があります。クイック リファレンス リストについては、「SSL VPN アクセスのためのユーザの設定 (130 ページ)」を参照してください。

10 「**SP L3 設定**」を選択します。

11 「**WLAN トンネル インターフェース**」ドロップダウン リストからインターフェースを選択します。WLAN トンネル インターフェースは既に設定されている必要があります。これを設定するには、「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページの「**インターフェースの追加**」フィールドで「**WLAN トンネル インターフェース**」を選択します。詳細については、*SonicOS 6.5 システム設定*を参照してください。

12 「**OK**」を選択します。

12

SSL VPN ウェブポータルの設定

SSL VPN > ポータル設定ページでは、SSL VPN 仮想オフィス ウェブ ポータルの外観と機能を設定できます。仮想オフィス ポータルは、NetExtender を起動するために (またはブックマークを選択して内部リソースにアクセスするために) ユーザがログインするウェブ サイトです。カスタマイズによって、どんな既存の企業ウェブ サイトやデザイン スタイルにも合わせることができます。

トピック:

- ポータル設定
- ポータル ロゴ 設定

ポータル設定

ログインしようとするユーザから見える内容がポータル設定によってカスタマイズされます。会社の要件に応じてオプションを設定してください。

オプション	定義
ポータル サイト タイトル	このフィールドには、ポータル ページのトップ タイトルとして表示するテキストを入力します。既定は、「**SonicWall - 仮想オフィス**」です。
ポータル バナー タイトル	このフィールドには、ページ最上部のロゴの隣に表示するテキストを入力します。既定は、「**仮想オフィス**」です。
ホームページ メッセージ	NetExtender アイコンの上に表示するメッセージの HTML コードを入力します。独自のテキストを入力するか、「**サンプル テンプレート**」を選択して既定のテンプレートに基づいてフィールドの内容を設定し、それをそのまま使うか編集します。ホーム ページ メッセージの体裁を確認するために「**プレビュー**」を選択します。
ログイン メッセージ	仮想オフィスへログインしようとするユーザに表示するメッセージの HTML コードを入力します。独自のテキストを入力するか、「**サンプル テンプレート**」を選択して既定のテンプレートに基づいてフィールドの内容を設定し、それをそのまま使うか編集します。ログイン メッセージの体裁を確認するために「**プレビュー**」を選択します。

次の設定は、仮想オフィス ポータルの機能をカスタマイズするものです。

- **ログイン後に NetExtender を起動する** - ユーザのログイン後に自動的に NetExtender を起動します。このオプションは、既定では選択されていません。
- **証明書のインポート ボタンを表示する** -「**仮想オフィス**」ページに「**証明書のインポート**」ボタンを表示します。これにより、ファイアウォールの自己署名証明書をウェブ ブラウザにインポートする処理が開始されます。このオプションは、既定では選択されていません。

  メモ：このオプションは、「**SSL VPN > サーバ設定**」ページの「**証明書の選択**」ドロップダウン メニューで、「**自己署名証明書を使用**」が選択されている場合に、Windows を搭載する PC 上の Internet Explorer ブラウザにのみ適用されます。

- **キャッシュ制御のための HTTP メタ タグを有効にする (推奨)** - ウェブ ブラウザに「**仮想オフィス**」ページをキャッシュしないように指示する HTTP タグを挿入します。このオプションは、既定では選択されていません。

  メモ：SonicWall では、このオプションを有効にすることを推奨しています。

- **SSL VPN ポータルに UTM 管理リンクを表示する (推奨しません)** - SSL VPN ポータルに SonicWall 装置の管理リンクを表示します。このオプションは、既定では選択されていません。

  重要：SonicWall では、このオプションを有効にすることを推奨しません。

ポータル ロゴ 設定

このセクションでは、仮想オフィス ポータルの最上部に表示されるロゴを構成するための設定について説明します。

- **既定のポータル ロゴ** - 既定のポータル ロゴ (SonicWall ロゴ) を表示します。

- **既定の SonicWall ロゴを使用する** - このチェックボックスをオンにすると、装置で提供されている SonicWall ロゴが使用されます。このオプションは、既定では選択されていません。
- **個別ロゴ (ロゴの URL を入力)** - 表示するロゴの URL を入力します。

  ヒント：ロゴは、155X36 サイズの GIF 形式でなければならず、透明または薄い背景色が推奨されます。

13

仮想オフィスの設定

「**SSL VPN > 仮想オフィス**」ページでは、SonicOS 管理インターフェースの内部に仮想オフィス ウェブポータルが表示されます。

トピック:

- 仮想オフィス ポータルへのアクセス
- NetExtender の使用
- SSL VPN ブックマークの設定

仮想オフィス ポータルへのアクセス

仮想オフィス ポータルには、2 つの方法でアクセスできます。システム管理者は、装置インターフェースを通じてアクセス可能で、サイト全体に適用される変更を行う権限を持ちます。ユーザはそれとは異なる手順でアクセスし、ユーザ自身の特定のプロファイルに影響する変更しか行うことができません。

システム管理者がSSL VPN 仮想オフィス ポータルにアクセスするには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」の「**SSL VPN > 仮想オフィス**」を選択します。

ユーザがSSL VPN 仮想オフィス ウェブ ポータルを表示するには、以下の手順に従います。

1 ファイアウォールの IP アドレスに移動します。

2 ログインページの下部にあるリンク「**SSLVPN へのログインは、ここを選択します**」を選択します。

NetExtender の使用

SonicWall NetExtender は、リモート ユーザがリモート ネットワークにセキュアな方法で接続できるようにする透過的なソフトウェア アプリケーションです。NetExtender により、リモート ユーザはリモート ネットワーク上の任意のアプリケーションを安全に実行できます。ファイルのアップロード/ダウンロード、ネットワーク ドライブのマウント、リソースへのアクセスといった作業がローカル ネットワークにいる感覚で行えます。NetExtender の接続では、ポイント ツー ポイント プロトコル (PPP) 接続を使用します。仮想オフィス ポータルには、NetExtender クライアントをダウンロードするためのリンクが表示されます。

ユーザは、次の 2 通りの方法で NetExtender にアクセスできます。

- SonicWall セキュリティ装置によって提供される仮想オフィス ポータルにログインし、NetExtender ダウンロード リンクを選択し、NetExtender をインストールして起動する。
- スタンドアロンの NetExtender クライアントを起動する。仮想オフィス ポータルから NetExtender をダウンロードして初めてインストールした後、他のクライアント アプリケーションと同様に、ユーザの PC から NetExtender に直接アクセスできます。

NetExtender は、起動時にポップアップ ウィンドウを表示します。SonicWall サーバには、NetExtender を最初に起動してクライアントをダウンロードするときに使用されるサーバが事前に設定されています。このドメインには、対応するドメインも設定されます。ユーザはユーザ名とパスワードを入力し、「**接続**」を選択します。

接続が確立されると、NetExtender ウィンドウに 3 つの画面が表示されます。「**状況**」、「**ルート**」、および「**DNS**」です。「**状況**」画面には、サーバ、クライアント IP アドレス、送受信されたキロバイト数、およびスループット (バイト/秒) が表示されます。「**ルート**」画面には、送信先サブネット IP アドレスおよび対応するネットマスクが表示されます。「**DNS**」画面には、DNS サーバ、DNS サフィックス、および WINS サーバが表示されます。ルートと DNS 設定は、SonicWall 装置の SonicOS 管理者によって制御されます。

ユーザは、接続が確立されたら NetExtender ウィンドウを閉じることができます。接続は開いたままになりますが、ウィンドウは最小化され、システム トレーから再度開くことができます (Windows の場合)。

NetExtender の詳細については、「NetExtender について (127 ページ)」を参照してください。

SSL VPN ブックマークの設定

仮想オフィス ホームページに表示する、ユーザ ブックマークを定義できます。ユーザは管理者の作成したブックマークを変更または削除することはできません。

ブックマークの作成の際、サービスによっては、非標準ポートで動作するものや、接続時にパスを要求するものがあることに注意が必要です。ブックマークの設定の際、**サービス種別**と**ホスト名または IP アドレス**の正しい形式とを合わせる必要があります。これらのオプションを設定する場合、次のテーブルを参照してください。

メモ：SonicOS 6.5 には、ActiveX と Java のサービス種別は存在しません。アップグレードの最中に、古いバージョンのプリファレンスが HTML5 に変換されます。

サービス種別に対するブックマーク名または IP アドレスの形式

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
RDP - ActiveX RDP - Java	IP アドレス	10.20.30.4
	IP: ポート (非標準)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
VNC	IP アドレス	10.20.30.4
	IP: ポート (セッションへ割り当て済み)	10.20.30.4:5901 (セッション 1 へ割り当て済み)
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
	メモ：ポートの代わりにセッション番号または表示番号を使用しないでください。	**メモ：**10.20.30.4:1 を使用しないでください。 **ヒント：**Linux サーバへのブックマークについては、この表の下にヒントがあります。
Telnet	IP アドレス	10.20.30.4
	IP:ポート (非標準)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC
SSHv1 SSHv2	IP アドレス	10.20.30.4
	IP:ポート (非標準)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	ホスト名	JBJONES-PC

重要：Linux サーバへの**仮想ネットワーク コンピューティング (VNC)** ブックマークを作成するときは、「**ホスト名または IP アドレス**」フィールドで、Linux サーバの IP アドレスとともにポート番号とサーバ番号を **ipaddress:port:server** の形式で指定する必要があります。例えば、Linux サーバの IP アドレスが 192.168.2.2、ポート番号が 5901、サーバ番号が 1 の場合は、「**ホスト名または IP アドレス**」フィールドに **192.168.2.2:5901:1** を指定します。

ポータル ブックマークを追加するには、以下の手順に従います。

1 「**管理 | 接続性 | SSL VPN > ポータル オフィス**」ページに移動します。

2 「**追加**」を選択します。

3 わかりやすいブックマーク名を「**ブックマーク名**」フィールドに入力します。

4 LAN 上のホスト コンピュータの完全修飾ドメイン名 (FQDN) または IPv4 アドレスを「**名前または IP アドレス**」フィールドに入力します。所定の**サービス**種別で想定される**名前または IP アドレス**の例については、「サービス種別に対するブックマーク名または IP アドレスの形式」テーブルを参照してください。

5 適切なサービスの種類を「**サービス**」ドロップダウン リストで選択します。

- **RDP (HTML5-RDP)**
- **SSHv2 (HTML5-SSHv2)**
- **TELNET (HTML5-TELNET)**
- **VNC (HTML5-VNC)**

選択によって表示が変わります。

6 選択したサービスに適した情報を残りのフィールドへ入力します。オプションおよび定義については、以下のテーブルを参照してください。

サービスが RDP (HTML5-RDP) に設定されている場合、以下の設定を行います。

画面サイズ	ドロップダウン メニューで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。 画面サイズはコンピュータによって異なるので、リモート デスクトップ アプリケーションを使用するときは、リモート デスクトップ セッションの実行元のコンピュータ画面のサイズを選択する必要があります。
画面の色	ドロップダウン メニューで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。

アプリケーションおよびパス (オプション)	必要であれば、リモート コンピュータ上のアプリケーションが存在するローカル パスを入力します。
次のフォルダから開始 (オプション)	必要であれば、アプリケーション コマンドを実行するローカル フォルダを入力します。
ウィンドウ詳細オプションの表示	矢印をクリックして拡張し、ウィンドウ詳細オプションの全体を表示します。有効化が必要なチェックボックスをオンにします。 • **クリップボードをリダイレクトする** • **自動再接続** • **ウィンドウ ドラッグ** • **オーディオをリダイレクトする** • **デスクトップ背景** • **メニューとウィンドウ アニメーション**
自動的にログインする	自動ログイン チェックボックスをオンにします。選択する場合、以下のどちらの認証情報を使用するか選択します。 • **SSL-VPN アカウント認証情報を使用する** • **個別認証情報を使用する** 個別認証情報を使用することを選択した場合、ユーザ名、パスワード、ドメインに、個別認証情報を入力します。 **メモ：**ユーザ名とドメインには、動的変数を使用できます。次の表 (動的変数) を参照してください。
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが SSHv2 (HTML5-SSHv2) に設定されている場合、以下を設定してください。	
自動的にホスト キーを受け入れる	有効にする場合、チェックボックスをオンにします。
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが TELNET (HTML5-TELNET) に設定されている場合、以下を設定してください。	
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが VNC (HTML5-VNC) に設定されている場合、以下を設定してください。	
表示のみ	ブックマークを表示のみモードにする場合はチェックボックスをオンにします。
デスクトップ共有	デスクトップ共有機能を有効にします。
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。

7 「**OK**」を選択して設定を保存します。

動的変数

用途	変数	使用例
ログイン名	%USERNAME%	US\%USERNAME%
ドメイン名	%USERDOMAIN%	%USERDOMAIN\%USERNAME%

第 3 部

接続性 | アクセス ポイント

- SonicWall アクセス ポイントについて
- アクセス ポイント ダッシュボード
- アクセス ポイント基本設定
- アクセス ポイント フロア プラン
- アクセス ポイントのファームウェアの管理
- アクセス ポイント トポロジ表示
- アクセス ポイント侵入検知サービスの設定
- 高度な IDP を設定する
- アクセス ポイントパケット キャプチャ
- 仮想アクセス ポイントの設定
- FairNet の設定
- Wi-Fi マルチメディアの設定
- アクセス ポイント 3G/4G/LTE WWAN
- Bluetooth LE デバイスの表示

14

SonicWall アクセス ポイントについて

SonicWall SonicPoint と SonicWave は、SonicWall セキュリティ装置と連携して企業全体で無線アクセスを提供することに特化して設計された無線アクセス ポイントです。インターフェースの「**管理**」表示の「**接続 | アクセス ポイント**」で、装置に接続されたアクセス ポイントを管理することができます。

メモ：SonicOS 6.5.3 以降では、「**管理 | システム セットアップ | 装置 > 基本設定**」ページの「**無線制御モード**」が「**フル機能ゲートウェイ**」または「**無線制御のみ**」に設定されているとき、**アクセス ポイント**のページが表示されます。「**無線なし**」が「**無線制御モード**」で有効になっている場合、「**アクセス ポイント**」メニューの見出しとその下のページは表示 ***されません***。詳細については、『*SonicOS 6.5 システム設定* 管理ガイド』を参照してください。

このセクションでは、SonicWall アクセス ポイント をネットワークで使用する際の情報とベスト プラクティス、および、SonicWall ネットワーク装置と統合する方法について説明します。

トピック:

- アクセス ポイントの機能の一覧
- アクセス ポイント機能
- 計画と実地調査
- アクセス ポイント配備のためのベスト プラクティス
- アクセス ポイントのライセンス
- SonicPoint/SonicWave の管理を始める前に
- アクセス ポイントと RADIUS アカウント

アクセス ポイントの機能の一覧

SonicOS にはさまざまな機能がありますが、SonicWall アクセス ポイントの種別によってサポート対象機能が異なります。次の対応表を参照してください。

アクセス ポイントの種別ごとの無線機能のサポート

機能名	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
帯域誘導	はい	はい	はい	**いいえ**
エア タイム フェアネス	はい	はい	はい	**いいえ**
無線検査パケット キャプチャ	はい	**いいえ**	**いいえ**	**いいえ**
WDS AP サポート	はい	はい	はい	**いいえ**
フロア プランの表示	はい	はい	はい	はい

アクセス ポイントの種別ごとの無線機能のサポート

機能名	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
トポロジ表示	はい	はい	はい	はい
SSLVPN コンセントレータ	はい	はい	はい	はい
リアルタイム監視の可視化	はい	はい	はい	いいえ
動的 VLAN	はい	はい	はい	いいえ
3G/4G/LTE Extender	はい	はい	はい	いいえ
クライアントのフィンガープリンティングとレポート	はい	はい	はい	いいえ
SNMP MIB の拡張	はい	はい	はい	はい
GRE 管理マルチコア サポート	はい	はい	はい	はい
Restful API のサポート	はい	はい	はい	いいえ
ゲスト サービス: IP ベースのゲスト認証バイパス ネットワーク	はい	はい	はい	はい
ゲスト サービス: ゲスト ユーザ グループのサイクル クォータ	はい	はい	はい	はい
ネイティブ ブリッジのサポート	はい	はい	はい	はい
ビルトイン無線リピータ モード	TZ Wireless の場合のみ	TZ Wireless の場合のみ	TZ Wireless の場合のみ	TZ Wireless の場合のみ
ビルトイン無線 WDS モード	TZ Wireless の場合のみ	TZ Wireless の場合のみ	TZ Wireless の場合のみ	TZ Wireless の場合のみ
IEEE 802.11s メッシュ ネットワーク	はい	いいえ?	いいえ?	いいえ?
Bluetooth 低消費電力 (BLE)	はい	いいえ?	いいえ?	いいえ?
Capture Security Center 報告	はい	いいえ?	いいえ?	いいえ?
無線クラウド管理のサポート	はい	いいえ	いいえ	いいえ

アクセス ポイント機能

SonicWall アクセス ポイント は SonicWall 次世代ファイアウォールと統合されて、総合的な有線および無線ネットワークに対する保護を提供する安全な無線ソリューションとなります。信号の品質と信頼性を高めた高速無線アクセスを提供し、最新の機能によってギガビット無線パフォーマンスを実現できます。SonicPoint/SonicWave シリーズは、IEEE 802.11a/b/g/n/ac 標準をサポートすることによって、高密度の環境でも、信号の劣化なしに広帯域を必要とするモバイルアプリケーションをご利用いただけます。

トピック:

- SonicPoint/SonicWave 機能
- 認証と準拠
- アクセス ポイントフロア プラン表示
- アクセス ポイント トポロジ表示
- 侵入検知/防御

- 仮想アクセス ポイント
- アクセス ポイント WMM 設定
- 日本版および国際版アクセス ポイントのサポート

SonicPoint/SonicWave 機能

SonicPoint/SonicWave アクセス ポイントは、より多くのアンテナ、より広域なチャンネル、より多くの空間ストリーム、そしてスループットと信頼性を向上させるその他の機能を提供することで、5 GHz 帯におけるより高速なスループットを実現します。SonicPoint AC および SonicWave 機器は、5GHz と 2.4GHz の両方の無線帯域をサポートし、以下のような重要な技術要素を持っています。

- **広域チャンネル** - 従来の 20 / 40 MHz チャンネルを引き続きサポートしながら、802.11ac 無線モジュール用の 80 MHz 帯チャンネルも使用します。これにより、チャンネル幅に関するパケットごとの動的なネゴシエーションが可能になり、干渉発生時に SonicWave は一時的に 40 または 20 MHz チャンネルにフォールバック可能。
- **最大 4 つの空間ストリーム** - 空間ストリームを追加すると、それに比例してスループットが向上します。2 ストリームで、スループットは単一ストリームの 2 倍になります。4 ストリームでは、4 倍のスループットが得られます。
- **複数ユーザ MIMO** - 多入力多出力空間分割多重化により、複数の独立したデータ ストリームの同時送受信が提供されます。

  SonicWave および SonicPoint AC はスループットを向上させることで、無線ディスプレイ、HDTV、大容量ファイルのダウンロード、構内や講堂での使用にさらに適した製品となっています。
- **レイヤ 3 管理フェーズ 1** - レイヤ 3 ネットワークへの アクセス ポイント の配備をサポートする DHCP およびトンネリング ソリューションを提供します。
  - SonicWall の DHCP ベース検出プロトコル (SDDP: SonicWall DHCP-based Discovery Protocol) は、よく知られた DHCP プロトコルをベースとし、 ゲートウェイと アクセス ポイント の双方がレイヤ 3 ローカル ネットワーク越しに互いを自動的に検出できるようにします。
  - リモート ネットワーク管理プロトコルである SonicWall の SSL VPN ベース管理プロトコル (SSMP: SonicWall SSL VPN-based Management Protocol) は、SonicWall SSL VPN インフラをベースとしており、アクセス ポイント を SSL VPN 対応のネットワーク セキュリティ装置によってインターネットを介して管理することを可能にします。
- **動的周波数選択 (DFS) のサポート** - DFS 証明書が発行されると、アクセス ポイント は動的周波数選択をサポートします。これにより、取り扱いに慎重を要する 5GHz 周波数帯のチャンネル内に、アクセス ポイント を配備することが可能となります。
- **アクセス ポイントダッシュボード** - **アクセス ポイント>ダッシュボード** ページは、個別のアクセス ポイントごとの統計を表示します。**ダッシュボード**には、帯域幅とクライアント情報のグラフィック形式による要約が表示されます。また、リアルタイムのクライアント監視詳細も提供します。
- **帯域ステアリング** - 帯域ステアリングにより、アクセス ポイント は5GHz に対応したクライアントに 5GHz 帯を使用させます。通常、5GHz 帯は干渉やトラフィックがより少なくなります。ただし、信号に干渉があるか、強度が 2.4GHz 帯より弱い場合、クライアントに 2.4GHz 帯を使用させます。全体の容量、スループット、およびユーザ エクスペリエンスを改善することを意図しています。

- **オープン認証、ソーシャル ログイン、および LHM** - SonicOS 6.2.7 以降では、フェイスブック、ツイッター、グーグル + などのソーシャル メディアでオープン認証とソーシャル ログインをサポートしています。ライトウェイト ホットスポット メッセージング (LHM) もサポートしています。
- **無線周波数解析** - 無線周波数解析 (RFA) は、アクセス ポイント やその他の近隣無線アクセス ポイントでの無線チャンネルの利用状況を、ネットワーク管理者が把握できるようにするための機能です。
- **SonicWave の個別設定の保持** - 削除または再同期された後もそれぞれの設定の一部を保持するように、アクセス ポイント プロファイルを設定することができます。
- **VLAN タグ付け** - SonicPoint/SonicWave は同一の VLAN ID を用いることで VAP が VLAN と接続するように設定されることを許可するので、仮想アクセス ポイント (VAP) を越えて VLAN 内の優先順位付けが可能です。 VLAN トラフィックに対する優先順位はファイアウォール アクセス ルールを通して設定可能です。
- **無線診断** - アクセス ポイント は重要な実行時データを収集して、それを永続的なストレージに保存することができます。アクセス ポイント に障害が発生した場合、アクセス ポイント の再起動時にそのデータを SonicWall 管理装置が取得して、それをテクニカル サポート レポート (TSR) 内に組み入れます。その後の アクセス ポイント の障害により、データは上書きされます。
- **アクセス ポイント 3G/4G WWAN** - ユーザは USB モデム装置を SonicWall アクセス ポイント に接続することができます。アクセス ポイントは、ダイアルアップでインターネットに接続する動作を実行できます。接続すると、アクセス ポイント はファイアウォールの WWAN 装置として機能し、WAN アクセスを提供します。
- **デイジー チェーン接続** - デイジー チェーン接続により、小規模な環境 (つまり、低密度のスイッチ インフラ) において、最小限のスイッチ ポートを使用しつつ複数の アクセス ポイント を配備することができます。例えば、店舗全体に分散する多数の機器を、店舗のスイッチ インフラに接続する場合が挙げられます。スイッチ インフラは、スイッチ ポートの密度と可用性という点では小規模ですが、店舗全体を網羅する複数のアクセス ポイントを含みます。アクセス ポイント は、LAN2 インターフェースを介してデイジー チェーン接続されます。

  重要：デイジー チェーン接続は、スループットに影響を与えます。1 台追加するごとに、スループットは低下します。スループットの重要性に基づいて、以下のようにします。
  - スループットが重要である場合は、次のようにして許容レベルのスループットを確保します。
    - SonicPoint N2 の場合は、デイジー チェーン接続するアクセス ポイントは 3 台までとします。
    - SonicPoint ACe/ACi の場合は、デイジー チェーン接続するアクセス ポイントは 2 台までとします。
  - スループットが重要でない場合でも、デイジー チェーン接続するアクセス ポイントは 4 台までとします。

  SonicWave または SonicPoint AC モデルと、SonicPoint N または N2 のモデルが混在する場合は、SonicWave または SonicPoint AC モデルをデイジー チェーンの先頭に配置します。
- **無線クラウド管理のサポート** - WCM を使用すると、SonicWave アクセス ポイントを中央のファイアウォールまたはクラウドから管理できます。WCM クラウドベースのインフラストラクチャにより、どこからでも Wi-Fi の問題にアクセス、制御、トラブルシューティングできます。

認証と準拠

SonicWall アクセス ポイント は厳しいテストに合格し、業界の認証を受けています。

Wi-Fi Alliance による認証

メモ：SonicPoint Dual Radio (SonicWave、SonicPoint NDR と SonicPoint ACe/ACi/N2) は、Wi-Fi Alliance による Wi-Fi 認証を受けていることを表す Wi-Fi CERTIFIED ロゴを取得しています。

Wi-Fi CERTIFIED ロゴは、Wi-Fi Alliance の認証マークです。このロゴを持つ製品は、Wi-Fi Alliance による厳しいテストを受け、Wi-Fi CERTIFIED を持つ他社製品を含む他の製品との相互運用性が確認されています。

FCC U-NII の新しい規則への準拠

バージョン 9.0.1.0-2 以降のファームウェアを実行している SonicWave および SonicPoint ACe/ACi/N2 で、FCC U-NII (Unlicensed -National Information Infrastructure) による新しい規則 (Report and Order ET Docket No. 13-49) がサポートされます。動的周波数選択 (DFS) に関する FCC の新しい規則に準拠するために、SonicPoint/SonicWave アクセス ポイントは DFS バンドのレーダー信号を検出してレーダー信号との干渉を回避します。

メモ：FCC の新しい規則に準拠したファームウェアを使用して製造された SonicPoint ACe/ACi/N2 無線アクセス ポイントは、SonicOS 6.2.5.1 以降でのみサポートされています。それより古い SonicPoint ACe/ACi/N2 アクセス ポイントは、SonicOS6.5 が稼働しているファイアウォールに接続すると、FCC の新しい規則に準拠したファームウェアに自動更新されます。

RED 準拠と認証

SonicWall TZ および SOHO 無線装置、ならびに SonicWall 無線アクセス ポイントは、欧州連合の無線機器指令 (RED) への適合性が確認されています。SonicWall 技術文書のサポート ポータル内にある、*無線機器指令 (RED) 補遺* を参照してください。
https://www.sonicwall.com/ja-jp/support/Technical-Documentation/Radio-Equipment-Directive-(RED)-Addendum

アクセス ポイントフロア プラン表示

SonicOS 6.5 では、多数の SonicWall アクセス ポイント 機器を管理するために視覚的なアプローチが可能です。また、物理的な位置とリアルタイムの状況も追跡できます。

SonicOS のフロア プラン表示は、実際の アクセス ポイント 無線配備環境をリアルタイムで図示します。新規の配備による無線通信範囲を推定するうえで役立ちます。フロア プラン表示はまた、コンテキスト メニューから、リアルタイムの状態監視、アクセス ポイント設定、アクセス ポイント除去、さらに RF 範囲の表示も提供します。

アクセス ポイント トポロジ表示

アクセス ポイントは、トポロジ表示から管理できます。トポロジ表示は、SonicWall ファイアウォールからエンド ポイントまでのネットワーク トポロジを表示します。アクセス ポイント のリアルタイムの状態を監視できます。コンテキスト メニューは、設定オプションも提供します。

この機能により、すべての WLAN 関連機器間の論理的関係性を表示し、トポロジ表示から装置を直接管理できます。「**接続 | アクセス ポイント > トポロジ表示**」を開くと、ファイアウォールが認識している機器をつなげ、それらの関係を示す、樹形図が表示されます。

トポロジ表示管理では、管理者向けに WLAN ネットワークがグラフィカルに表示され、併せて最もよく使われる情報と状況が示されます。機器はツリー上のノードとして描画され、ツリーはマウスとマウス ホイールを使って拡大できます。樹形図に表示される情報には以下のものが含まれます。機器の種類、IP アドレス、接続されているインターフェース、名称、クライアント数、一部の機器については状態を示すための LED ランプ模擬表示。ツール チップのフキダシには、機器の詳細情報が表示されます。

侵入検知/防御

SonicWall アクセス ポイント は、無線周波数 (RF) 機器に対する保護を提供します。無線ネットワーク機器で使用される RF 技術は、侵入者のターゲットです。アクセス ポイント は直接 RF 監視によって、無線または有線ネットワークの現在の運用を中断することなく脅威を検出します。当該の機能には以下を含みます。

- **侵入検知サービス** - 侵入検知サービス (IDS) により、SonicWall ネットワーク セキュリティ装置は、一般的な種類の不正な無線アクティビティを認識して対応策を講じることができます。IDS は、ファイアウォールがアクセス ポイント上の 802.11a/b/g/n/ac の 無線帯域をスキャンすることによって検出可能なすべてのアクセス ポイントについて報告します。
- **高度な侵入検知と防御** - 高度な侵入検知と防御 (IDP) は、電波スペクトルを監視して、許可されていないアクセス ポイントの存在を検知 (侵入検知) し、自動的に防止策を実行 (侵入防御) します。アクセス ポイントで高度な IDP を有効にすると、無線機能は専用の IDP センサーとして機能します。
- **悪意のある機器の検知と防御** - SonicOS 6.5.3 以降では、スキャン無線を備えたアクセス ポイントは、無線アクセス ポイントとして機能し続けながら、悪意のあるデバイスを検出するセンサーとして機能します。6.5.3 より前は、悪意のある機器の検知と防御に焦点を当てた専用センサー モードに、2.4GHz と 5GHz 両方の帯域で受動的または事前予防的にアクセス ポイントを設定することが可能です。片方しか使っていない場合でも、両方の帯域をスキャン可能です。悪意のある機器は、ネットワークに接続されているか、またそれが有線または無線メカニズムによって遮断されているかどうかをレポートするために分析することが可能です。
- **内蔵無線機のスキャン スケジュール** - アクセス ポイントは、侵入検知/防御スキャンの実行を、最大で週 7 日、1 日 24 時間にわたる、きめ細かなスケジュール オプションによってスケジュールできます。「**IDS スキャンをスケジュールする**」オプションは、すべてのアクセス ポイント モデルのアクセス ポイント プロファイルを編集するときに、「**無線 0/1 詳細**」または「**詳細**」画面で使用できます。

仮想アクセス ポイント

仮想アクセス ポイント (VAP) とは、単一の物理 アクセス ポイント を多重インスタンス化することにより、単一の アクセス ポイント を複数の別個の アクセス ポイント または VAP として見せるもので

す。実際には物理 アクセス ポイント は 1 つしかないにもかかわらず、無線 LAN のクライアントにとっては、各 VAP が独立した物理アクセス ポイントのように見えます。

- **仮想アクセス ポイント スケジュール サポート** - 使いやすくするために、各仮想アクセス ポイントのスケジュールを個別に有効/無効にすることが可能になりました。
- **仮想アクセス ポイント レイヤ 2 ブリッジ** - 各 VAP を、LAN ゾーン上の対応する VLAN インターフェースにブリッジして、さらなる柔軟性を提供することが可能です。
- **仮想アクセス ポイント ACL サポート** - 各 VAP が、より効率的な認証制御を提供するために、個別のアクセス制御リスト (ACL) をサポートすることが可能です。
- **SonicPoint N Dual Radio 上の仮想アクセス ポイント グループ共有** - デュアル無線に対して同じ VAP/VLAN 設定を適用することが可能です。これにより、両方の無線に対して統一されたポリシーを使い、そしてネットワーク スイッチ内の VLAN トランクを共有することが可能になります。

アクセス ポイント WMM 設定

アクセス ポイント アクセス ポイントは Wi-Fi マルチメディア (WMM) をサポートし、Wi-Fi 電話機上の VoIP や無線ネットワーク上のマルチメディア トラフィックといった多種多様なアプリケーションで、より優れたサービス品質を提供します。WMM は IEEE 802.11e 標準に基づく Wi-Fi Alliance の相互通信認証です。WMM は 4 つのアクセス種別 (音声型、映像型、最大努力型、バックグラウンド型) に基づいてトラフィックに優先順位を付けます。

メモ：WMM は保証されたスループットを提供しません。

それぞれのアクセス種別には自身の伝送キューがあります。WMM は、アクセス ポイント が複数の優先順位アクセス種別に対して複数のキューを実装することを必要とします。アクセス ポイントは、アプリケーションまたはファイアウォールが提供する IP データ内のサービス種別 (TOS) 情報に基づいて、トラフィック種別を区別します。TOS 提供の 1 つの方法は、ファイアウォール サービスとアクセス ルールを介し、もう 1 つは VLAN タグ付けを介します。

「**管理**」表示の「**接続 | アクセス ポイント > Wi-Fi マルチメディア**」ページは、WMM 設定および割付の設定方法を提供します。

日本版および国際版アクセス ポイントのサポート

SonicOS は、日本および国際的な SonicPoint ACe / ACi / N2 およびSonicWave 432e / 432i / 432o 無線アクセス ポイントの両方をサポートします。国際版 アクセス ポイント とは、米国と日本以外の国で配備され、動作するものです。

国際版アクセス ポイントを SonicWall ネットワーク セキュリティ装置に接続すると、SonicOS によって「**アクセス ポイント > 基本設定**」ページに「**登録**」ボタンが表示されます。「**登録**」を選択すると、該当する「**国番号**」を選択できるダイアログが表示されます。

メモ：必ず、アクセス ポイントを登録するユーザの所在国ではなく、アクセス ポイントが配備されている国の国番号を選択します。

カナダ以外の国番号で登録されている国際版 アクセス ポイント は、「**接続 | アクセス ポイント > 基本設定**」ページの プロファイルで国番号を変更できます。

重要：カナダの国番号で登録されている アクセス ポイント については、SonicWall サポートに問い合わせなければ国番号を変更することはできません。

計画と実地調査

SonicWall アクセス ポイント を実環境に配備する前に、ある程度時間をかけて装置の必要条件を理解してください。以下のセクションでは、配備に対する前提条件を説明し、実地調査の一環として確認すべき事項を明示します。

トピック:

前提条件

アクセス ポイントを適切に配備するための要件を次に示します。

- SonicOS は、アクセス ポイントのファームウェア イメージをダウンロードして更新するために、ネットワーク セキュリティ装置用にパブリック インターネット アクセスが必要です。パブリック インターネットにアクセスできない場合、アクセス ポイントのファームウェアを手動でダウンロードして入手する必要があります。
- 1 つ以上の SonicWall 無線アクセス ポイント。
- アクセス ポイントの電力供給に PoE/PoE+ スイッチを使用する場合は、次のいずれかを使用する必要があります。
  - SonicWave 432e/432i/432o の場合は、802.3at 準拠のイーサネット スイッチ
  - SonicPointACe/ACi/N2 の場合は、802.3at 準拠のイーサネット スイッチ
  - その他の アクセス ポイント モデルの場合は、802.3af 準拠のイーサネット スイッチ
- SonicWall ネットワーク セキュリティ装置だけでなく PoE/PoE+ スイッチについてもサポート契約を結ぶことを強くお勧めします。その契約によって、スイッチ側またはファイアウォール側に問題が検出された場合や、新機能がリリースされた場合に、新しいバージョンに更新することができるようになります。
- 設置の前に、設置と配備のために何を準備することが必要かを理解するために、完全な実地調査を必ず実施してください。
- 配線およびケーブル インフラストラクチャを調べ、SonicWall アクセス ポイント とイーサネット スイッチの間のエンド ツー エンド接続が CAT5、CAT5e、CAT6 のいずれかであることを確認します。
- 設置ポイントの建築基準を確認し、建物の設備担当者と相談して、目的の設置ポイントが基準に違反しないことを確認します。

実地調査と計画

実地調査を行って SonicWall アクセス ポイント 配備を計画することが、配備成功のために重要です。調査および計画にあたっては、以下のガイドラインを含めてください。

- アクセス ポイント を配備する予定のエリア全体を実際に歩いて回ります。無線スペクトラム スキャナを使用して、既存のアクセス ポイントや、それらがブロードキャストしているチャンネルがないか確認します。SonicWall は、現時点では、Fluke 社または AirMagnet 社の製品で実地調査を行うことをお勧めします。NetStumbler/MiniStumbler を試してみることもできます。 無料ツールですが妥当な測定機能を備えており、使用中の無線カードで動作する場合は使用できます。
- 実地調査の間に使用するため、施設の平面図を取得してください。施設の平面図を使用して、アクセス ポイント の場所と無線セルの範囲を書き込むと便利です。実地調査の結果として設計を新しくすることになる可能性もあるため、平面図は複数のコピーを取っておいてください。また、信号に影響を与える可能性のある壁、廊下、エレベータの場所も確認します。ユーザがいる場所といない場所を確認することができます。

  実地調査の間、干渉の原因となる可能性のある電子機器 (電子レンジ、CT スキャン装置、他) がないか確認してください。電子機器が多数設置されている区域では、使用する配線の種類も特定してください。
- 調査は三次元的に行います (左右に、前後に、そして左右に)。無線信号は上下階にも影響するためです。
- 電源と配線に基づいて アクセス ポイント の場所を決めます。金属製またはコンクリート製の壁の近くは避け、できる限り天井の近くに アクセス ポイント を配置します。
- 無線スキャン ツールを使用して、信号強度とノイズを調べます。信号/ノイズ比は、少なくとも 10dB 以上 (11Mbps 時の最小要件)、できれば 20dB が求められます。両方の要素がサービス品質に影響します。
- 実地試験の結果によっては、いくつかの アクセス ポイント の位置を変更して再テストを行う必要がある可能性もあります。
- 設定とログを保存し、後日参照できるように の場所を記録します。フロア プラン表示を構築するために、この情報が必要となります。
- 旧式の SonicPoint モデルを使用している場合は、特定の場所またはすべての場所で、競合する既存の 802.11b/g チャンネルが飽和状態になっている場合があります。その場合は、アクセス ポイント の配備に 802.11a 無線を使用することも検討できます。この場合、ブロードキャストできるチャンネル配列はずっと多くなりますが、802.11a の到達範囲には限界があり、また、それらの機器に外部アンテナを追加することはできません。
- 制御範囲外の場所に無線信号をブロードキャストしないようによく気をつけてください。 信号が漏出する可能性のある場所を調べ、アクセス ポイント を適宜調整します。
- 簡易使用の場合は、アクセス ポイント ごとに 15～20 ユーザとして計画できます。業務用の場合は、アクセス ポイント ごとに 5～10 ユーザとして計画してください。
- ローミングするユーザを考慮して計画を行います。そのためには、信号オーバーラップが最小になるように各 アクセス ポイント の強度を調整する必要があります。オーバーラップが顕著な場所で複数のアクセス ポイント が同じ SSID にブロードキャストすると、クライアントの接続の問題が頻出することがあります。
- SonicOS のスケジュール機能を利用して、不使用時には アクセス ポイント を停止してください。業務時間外 (例えば夜間や週末) には アクセス ポイント を稼働しないことをお勧めします。

PoE と PoE+

計画時に、アクセス ポイント を設置するケーブルの配線長を確認します。これは 100 メートル以内にする必要があります。PoE スイッチまたは SonicWall PoE 対応 TZ 装置を使用しない場合は、アクセス ポイント 用の電源アダプタ、または PoE インジェクタについても検討する必要があります。電気事故や火災の原因となる配線を行わないようにしてください。

配線長が長いと電力損失の原因となります。アクセス ポイント と PoE スイッチの間の配線長が 100 メートルあると、電力/信号は最大で 16% 低下することがあります。したがって、SonicPoint の動作を維持するために、 PoE スイッチはさらに大きな電力をポートに供給しなければならなくなります。

SonicPoint ACe/ACi/N2

SonicPoint ACe/ACi/N2 に PoE/PoE+ (Power over Ethernet/Power over Ethernet plus) を供給するスイッチはすべて、802.3at に完全に準拠する必要があります。非準拠のスイッチで SonicPoint を稼働しないでください。SonicWall はそれをサポートしていません。

重要：pre-802.3at 規格検出は、接続の問題の原因となる場合があるので、無効にします。

SonicPoint AC (Type 1) は、クラス 0、1、2、または 3 PD が設定可能です。SonicPoint AC (Type 2) は、クラス 4 PD に設定します。最小/最大電力出力値は以下のとおりです。

- Type 1、クラス 0 PD の使用電力は、最小 0.5 W、最大 15.4 W
- Type 1、クラス 1 PD の使用電力は、最小 0.5 W、最大 4.0 W
- Type 1、クラス 2 PD の使用電力は、最小 4.0 W、最大 7.0 W
- Type 1、クラス 3 PD の使用電力は、最小 7.0 W、最大 15.4 W
- Type 2、クラス 4 PD の使用電力は、最小 15.4 W、最大 30 W

重要：クラスが一致しないと、ハンドシェイクで混乱が発生し、SonicPoint アクセス ポイントが再起動されます。

各 SonicPoint ACe/ACi/N2 に必ず 25 W の供給が保証されるようにします。

特に注意すべき点は、すべての PoE/PoE+ スイッチが各 PoE ポートに最小 25 W の電力を供給できるようにすることです。例えば、SonicPoint ACe/ACi/N2 をサポートするポートには 25 W の電力が必要です。スイッチが各ポートにおいて、ポートあたり 25 W を保証できない場合は、外付けの冗長電源を追加する必要があります。PoE/PoE+ スイッチの製造元によく確認して、使用する全 PoE/PoE+ 機器を動作させるのに十分な電力がスイッチに供給されるようにする必要があります。

旧式の SonicPoint N/Ni/Ne/NDR

旧式の SonicPoint と SonicPoint N/Ni/Ne/NDR はクラス 0 PD に設定され、使用電力は最小 0.44W、最大 12.95W となります。

旧式の SonicPoint と SonicPoint N/Ni/Ne/NDR に PoE を供給するスイッチはすべて、802.3af に完全に準拠する必要があります。非準拠のスイッチで SonicPoint を稼働しないでください。SonicWall はそれをサポートしていません。

pre-802.3af 規格検出は、接続の問題の原因となる場合があるので、無効にします。

各ポートに 10 ワットの供給を確保し、PoE の優先度を重大または高に設定します。

アクセス ポイント配備のためのベスト プラクティス

このセクションでは、SonicWall の 無線アクセス ポイントのデザイン、設置、配備、設定の問題に関する SonicWall の推奨事項やベスト プラクティスについて説明します。こうした情報により、任意の規模の環境に アクセス ポイント を適切に配備できます。このセクションで示されるサードパーティ製イーサネット スイッチについては、SonicWall から直接テクニカル サポートを行うことはできません。

重要：このセクションに記載されているサードパーティ製イーサネット スイッチについては、SonicWall が直接テクニカル サポートを提供することはできません。また、SonicWall の関知しないところで変更が生じる可能性もあり、スイッチの製造元が新しいモデルやファームウェアをリリースした場合にはこのセクションの記載内容が無効になる可能性があります。

トピック:

インフラ内のスイッチ

SonicWall インフラ内には、ほとんどのスイッチを使用できます。ただし、最適なパフォーマンスを確実に得るためには、個別の設定またはプログラミングが必要な可能性があります。

テスト済みのスイッチ

以下のスイッチは、SonicWall アクセス ポイント についてテスト済です。個々に提供されているガイダンスに注意してください。

- Cisco - Cisco 製スイッチのほとんどは問題なく動作しますが、いくつかのモデルについていくつかの問題が発見されています。
  - SonicWall では SonicWall アクセス ポイント の配備に Cisco Express シリーズのスイッチを使用することを推奨していません。
  - SonicWall は、SonicPointACe/ACi/N2 のイーサネットが、Cisco 製スイッチ 2960X-PS-I に対して、省電力型イーサネットの互換性の問題があることを確認しています。SonicPoint 接続ポートに対して、EEE を無効にしてください。詳細については、以下の Cisco 書類を参照してください。
    http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-0_2_EX1/int_h

w_components/configuration_guide/b_int_152ex1_2960-xr_cg/b_int_152ex1_2960-xr_cg_chapter_01001.pdf。

- D-Link PoE スイッチ - 独自仕様のブロードキャスト制御およびストーム制御メカニズムをすべて無効にする必要があります。アクセス ポイント のプロビジョニングおよび収集メカニズムと干渉するからです。
- Dell - アクセス ポイント ポートで STP を高速起動に設定してください。
- Extreme - アクセス ポイント ポートで STP を高速起動に設定してください。
- Foundry - アクセス ポイント ポートで STP を高速起動に設定してください。
- HP ProCurve - アクセス ポイント ポートで STP を高速起動に設定してください。
- Netgear - SonicWall アクセス ポイント の配備に Netgear PoE スイッチを使用することはお勧めしません。

スイッチ プログラミングのヒント

以下のセクションでは、SonicWall インフラストラクチャにおいて、スイッチに使用するスイッチ命令サンプルを説明します。詳細については、適切なベンダー サンプルを参照してください。

Dell スイッチ設定のサンプル (インターフェースごと)

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (注:FCS エラーが発生する場合のみ)
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

D-Link スイッチ設定のサンプル

D-Link 製 PoE スイッチにはコマンド ライン インターフェースがないので、ウェブ インターフェースを使用する必要があります。

メモ：マルチキャストを使用する環境の場合は、推奨されるファームウェア バージョンを D-Link に確認してください。

これらのスイッチに SonicWall アクセス ポイント を追加する前に、スイッチのスパニング ツリー、ブロードキャスト ストーム制御、LLDP、およびセーフガード エンジンを無効にしてください。これらはいずれも アクセス ポイント のプロビジョニング、設定、および機能に影響する可能性があります。

HP ProCurve スイッチ コマンドのサンプル (インターフェースごと)

- 「link to SonicPoint X」(または SonicWave X) にリセット
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (注:グローバル コマンド)
- speed-duplex 100-half (注:FCS エラーが発生する場合のみ)
- spanning-tree *xx* admin-edge-port (注: *xx* はポート番号)
- mdix-mode mdix

配線に関する考慮事項

施設の組織と共同で、実装の際に配線に関するガイドラインが確実に考慮されるようにしてください。

- 配線は、CAT5、CAT5e、CAT6 のいずれかのエンド ツー エンドにします。
- SonicPoint AC 装置に対する 802.3af と 802.3at の信号制限に基づき、PoE スイッチと アクセス ポイント の間のイーサネット配線長は、100 メートルを超えてはいけません。
- 配線長が長くなるほど PoE の電力損失を考慮する必要があり、電力損失は最大 16% にも及ぶことがあります。配線長が長いほど、ポートに必要な電力供給も大きくなります。

チャンネル

SonicWall アクセス ポイント の既定の設定は、**自動チャンネル** になっています。この設定では、アクセス ポイント は起動時にスキャンを実行し、送信中の他の無線機器がないかを確認します。続いて、送信に使用するための未使用チャンネルを検索します。大規模な配備では、この設定では問題が発生する可能性があるため、アクセス ポイント ごとに固定チャンネルを割り当てることをお勧めします。

ヒント：SonicPoint/SonicWave とその MAC アドレスのダイアグラムを用意すると、オーバーラップの回避に役立ちます。施設の平面図に SonicPoint/SonicWave の場所と MAC アドレスを書き込むことをお勧めします。

SonicOS 6.5.3 以降では、IEEE 802.11 WLAN の SonicWave アクセス ポイントで動的チャンネル選択 (DCS) がサポートされています。DCS を使用すると、アクセス ポイントは次のことができます。

- 動作する最適なチャンネルを決定します。
- 基本サービスセット (BSS) に関連付けられているすべてのステーション (STA) を新しく選択されたチャンネルに切り替えます。

DCS では、アクセス ポイントは最適なチャンネルを継続的に監視し、RF 環境に応じて動的に変更します (干渉する隣接 AP とマイクロ波が送受信されるため)。チャンネルを変更すると、「**調査 | ログ > イベント ログ**」にログ エントリが生成されます。

スパニング ツリー

イーサネット ポートが電気的にアクティブになると、ほとんどのスイッチは、既定でそのポートのスパニング ツリー プロトコルを有効化し、ネットワーク トポロジにループがあるか確認します。この 50～60 秒の検出時間の間、ポートはトラフィックを通過させません。この機能は、SonicWall アクセス ポイント で問題が発生する原因となることがわかっています。

スパニング ツリーが必要ない場合は、スイッチでグローバルに無効にするか、SonicWall アクセス ポイント 機器に接続している各ポートで無効にします。それが不可能な場合は、スイッチの製造元に *高速スパニング ツリー検出* が可能かどうかを確認します。これは、接続の問題が発生しないようにスパニング ツリーを短時間で実行する方法です。これを行うためのプログラミング サンプルについては、「Dell スイッチ設定のサンプル (インターフェースごと)」を参照してください。

VTP および GVRP トランク プロトコル

これらのトランク プロトコルは、アクセス ポイントに直接接続しているポートでは無効にしてください。これらは SonicPoint で、特にハイエンドの Cisco Catalyst シリーズ スイッチを使用する場合に、問題の原因となることがわかっています。

ポート集約

多くのスイッチで、ポート集約は既定で有効になっており、それが原因でよく問題が起こります。ポート集約は、SonicWall アクセス ポイント に直接接続しているポートでは無効にする必要があります。PAGP/ファースト イーサチャンネル/イーサチャンネルも、SonicWall アクセス ポイント につながるポートでは無効にします。

ポートシールド

SonicPoint をポートシールドするには、それらの SonicWall アクセス ポイント を PortShield グループのメンバーとして設定します。それらの アクセス ポイント を X シリーズ スイッチに設定する場合は、所属する PortShield グループを専用リンクのポートとして設定しなければなりません。

ブロードキャスト スロットリング/ブロードキャスト ストーム

ブロードキャスト スロットリング/ブロードキャスト ストーム機能は、一部のスイッチ、特に D-Link で問題になります。できればポートごとに、それが不可能ならグローバルに無効にしてください。

速度と通信方式

速度と通信方式のオプションによっては、SonicWall アクセス ポイント に対して問題を発生する原因となる可能性があります。現時点では、SonicWall アクセス ポイント では、速度と通信方式の**自動ネゴシエーション**のみ使用できます。これらの問題を解決または回避するには、以下を検討してください。

- スイッチで速度と通信方式をロックし、アクセス ポイント を再起動すると、接続の問題が解消する場合があります。
- ポートにエラーがないか確認します。これは通信方式の問題がないかを調べる最善の方法です (ポートではスループットの低下も発生します)。

SonicPoint 自動プロビジョニング

トピック:

- 自動配布 (SDP と SSPP)
- 自動プロビジョニングの有効化

自動配布 (SDP と SSPP)

SonicWall ディスカバリ プロトコル (SDP) は、SonicPoint/SonicWave と SonicOS が動作している機器で使われているレイヤ 2 プロトコルです。SDP は、以下のメッセージを通じて SonicPoint/SonicWave 装置の自動プロビジョニングを行うための基盤です。

- **広告** - 通信相手を持たない SonicPoint/SonicWave 機器は、起動時および定期的に自分自身をブロードキャストによって告知 (広告) します。広告を受信した SonicOS 機器は、広告に含まれている情報に基づいて SonicPoint/SonicWave の状態を確認します。その後、SonicOS 機器は相対するすべての SonicPoint/SonicWave の状態を報告し、必要に応じて設定アクションを実行します。
- **検出** - SonicOS 機器は、L2 接続された SonicPoint/SonicWave 装置から応答を引き出すために、検出要求のブロードキャストを定期的に送信します。
- **設定指示** - SonicOS から特定の SonicPoint/SonicWave へのユニキャスト メッセージです。配布のための暗号化鍵を確立することと、設定モードを開始させるためのパラメータを設定することが目的です。
- **設定承認** - 設定指示に対する肯定応答として、SonicPoint/SonicWave から相手の SonicOS 機器に向けられたユニキャスト メッセージです。
- **キープアライブ** - SonicPoint/SonicWave から相手の SonicOS 機器へのユニキャスト メッセージで、SonicPoint/SonicWave の状態を確認するために使われます。

設定指示では、SDP 交換を通じて、SonicPoint/SonicWave がプロビジョニングまたは設定の更新を必要としていると SonicOS 機器が判断した場合 (例えば、チェックサムの不一致が発生した場合や、ファームウェアの更新がある場合)、3DES で暗号化された信頼性の高い TCP ベースの SonicWall シンプル プロビジョニング プロトコル (SSPP) チャンネルが使われます。SonicOS 機器は、このチャンネルを介して SonicPoint/SonicWave に更新を送信し、SonicPoint/SonicWave は更新された設定を使用して再起動します。SonicPoint/SonicWave から提供される状態情報は、検出およびプロビジョニング プロセスのどの段階でも SonicOS 機器上で確認できます。

自動プロビジョニングの有効化

SonicPoint 自動プロビジョニングを有効にすると、以下の無線 SonicPoint/SonicWave プロビジョニング プロファイルを自動的に配布することができます。

- SonicPoint
- SonicPoint N

- SonicPointNDR
- SonicPoint AC
- SonicWave

無線 SonicPoint/SonicWave の初期設定は、無線 LAN 管理ゾーンに付属している SonicPoint/SonicWave プロファイルからプロビジョニングされます。無線 SonicPoint/SonicWave のプロビジョニング後、このプロファイルは、どの アクセス ポイント とも直接には関連付けられないオフライン設定テンプレートとなります。そのため、プロファイルを変更しても、再プロビジョニングのために SonicPoint/SonicWave が自動的に始動されることはありません。

自動プロビジョニングが導入される前は、管理者がすべての SonicPoint を手動で削除してから、新しい SonicPoint をプロファイルに同期する必要があったため、作業に時間がかかりました。設定を簡素化し、管理のオーバーヘッドを減らすために、SonicPoint 自動プロビジョニングは導入されました。

個々の SonicPoint/SonicWave プロビジョニング プロファイルに対して自動プロビジョニングを有効にするチェックボックスは、**ネットワーク > ゾーン > 設定 > 無線** 設定ダイアログにあります。既定では、SonicPoint/SonicWave プロビジョニング プロファイルのチェックボックスがオンになっておらず、自動プロビジョニングも有効になっていません。

プロビジョニング プロファイルのチェックボックスがオンのときにプロファイルを変更すると、そのプロファイルにリンクされたすべての アクセス ポイント が再プロビジョニングおよび再起動され、新しい動作状態になります。

SonicPoint/SonicWave に対するリモート MAC アクセス制御

重要：「リモート MAC アドレス アクセス制御」オプションは、IEEE 802.11i EAP が有効になっている場合に同時に有効にすることはできません。IEEE 802.11i EAP が有効になっている場合に「リモート MAC アドレス アクセス制御」オプションを同時に有効にしようとすると、次のエラー メッセージが表示されます。

```
IEEE 802.11i EAP が有効化されている場合は､リモート MAC アドレス アクセス制御を設定できません。
```

メモ：リモート MAC アクセス制御は、仮想アクセス ポイントに対してもサポートされています。「リモート MAC アドレス アクセス制御の設定」を参照してください。

リモート RADIUS サーバにおいて、MAC ベースの認証ポリシーに基づく無線アクセス制御を強制することができます。手順については「リモート MAC アドレス アクセス制御の設定」を参照してください。

アクセス ポイントのライセンス

SonicWave アクセス ポイントのライセンスは、SonicPoint アクセス ポイントのライセンスとは異なります。

トピック:

SonicWave ライセンス

SonicWall では、個別の SonicWave 装置ごとに追加のライセンスが必要です。ライセンスがあると、SonicWall ファイアウォールから SonicWave を管理できます。SonicWave 装置には最初に 6 カ月の管理ライセンスがバンドルされています。

SonicWall ファイアウォールは、SonicWall ライセンス マネージャ (LM) からライセンス状況を取得し、SonicWave アクセス ポイントの管理機能を有効にします。ライセンスの有効期限終了の 30 日前になると、ライセンスの更新が必要であるという通知がファイアウォールからシステム管理者に送られます。

SonicWave ライセンスの有効期限が終了し、更新しなかった場合は、SonicWall ファイアウォールによってサービス停止処理が行われて SonicWave の管理が停止し、SonicWave アクセス ポイントはトラフィックをブリッジするアクセス ポイントとして機能しなくなります。MySonicWall からライセンス更新の支払い手続きを行うと、ライセンス マネージャで SonicWave のライセンスが延長されてファイアウォールが新しいライセンスが取得し、サービス再開処理が行われて SonicWave アクセス ポイントが再び有効になります。

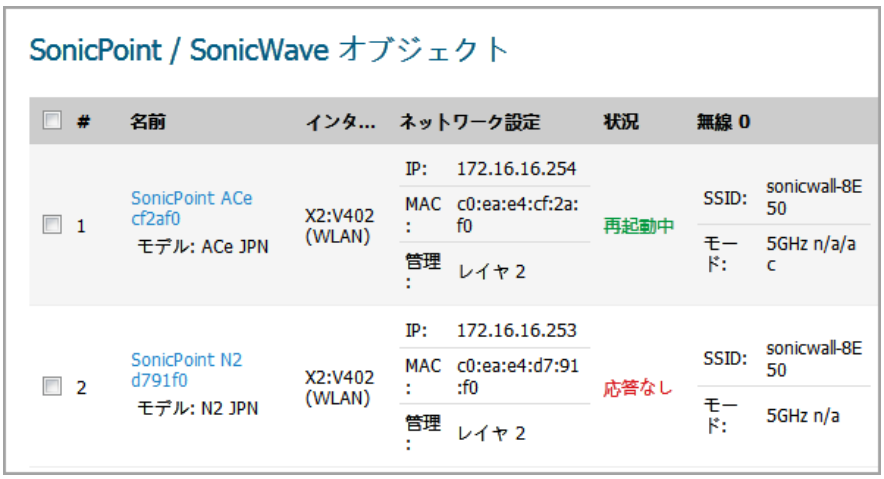
メモ：環境が隔離されていてファイアウォールでライセンス マネージャを使用できない場合は、管理者がファイアウォールに SonicWave ライセンス キーセットを入力することによって SonicWave のライセンス状況を変更できます。SonicWave に有効なライセンスがある限り、ファイアウォールで SonicWave を管理できます。ファイアウォールはライセンス マネージャとの間で SonicWave ライセンスを同期するライセンス プロキシの役割を果たします。

SonicWave アクセス ポイントに有効なライセンスが保持されている間のみ、SonicWave は通常のアクセス ポイントとして動作します。ライセンスが無効になると、有効なライセンス期間が延長されるまで、機能が停止します。

ライセンス状況

SonicWave ライセンスの状況を確認するには:

1. 「**接続 | アクセス ポイント > 基本設定**」ページに移動します。
2. 「SonicPoint/SonicWave オブジェクト」テーブルまで下にスクロールし、アクセス ポイントの「**状況**」を確認します。



SonicWave アクセス ポイントの状況は次のいずれかになっています。

- **利用可能** - 緑色の文字で、アクセス ポイントにライセンスがあることを示しています。

- **未購読** - 赤色の文字で、アクセス ポイントにライセンスがないことを示しています。
- **まもなく期限切れ** - 30 日以内にライセンスの有効期限が終了することを示しています。

手動によるライセンス更新

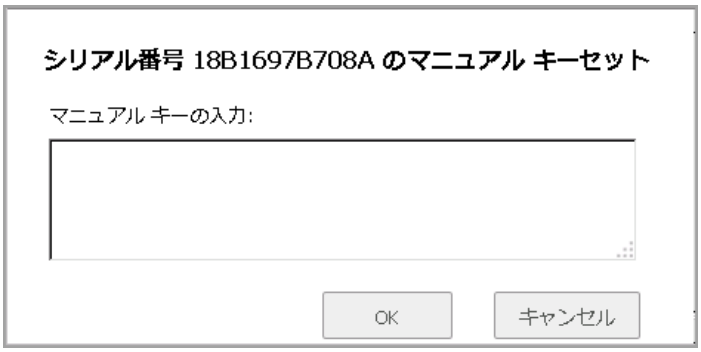
ファイアウォールでライセンス マネージャを使用して SonicWave ライセンスを更新できない場合も、GMS または SonicOS 管理インターフェースを使用して手動でライセンスの設定や更新を行うことができます。

1 MySonicWall にログインし、SonicWave ライセンスの手動キーセットを取得します。それをクリップボードにコピーします。

2 ファイアウォールで、「**管理 | 接続性 | アクセス ポイント > 基本設定**」に移動します。

3 「**SonicPoint/SonicWave オブジェクト**」まで下にスクロールします。

4 手動で更新する SonicWave の「設定」列にある解錠アイコンを選択します。



5 キー フィールドにライセンス キーを入力し、「**OK**」を選択します。

ファイアウォールで、SonicWave アクセス ポイントの新しいライセンス キーを更新する処理が開始します。SonicWave アクセス ポイントは、更新されたライセンス キーを保存し、無線インターフェースを起動し、トラフィックのブリッジを再開し、コンソール アクセスをオープンします。

ライセンスの自動更新

ファイアウォールでは、定期的に SonicWave アクセス ポイントへの自動問い合わせが行われます。SonicWave アクセス ポイントが更新されていた場合、ファイアウォールは新しいライセンスの有効期限をピア リストに記録し、SonicWave アクセス ポイントの新しいライセンス キーセットを更新し、これを反映して機能を制御します。

SonicPoint/SonicWave の管理を始める前に

SonicOS 管理インターフェースで SonicPoint/SonicWave を管理するにはまず、次の項目を実行する必要があります。

1 アクセス ポイント のプロビジョニング プロファイルの設定

2 無線ゾーンを設定します。

3 無線ゾーンにプロファイルを割り当てます。この手順はオプションです。ゾーンに既定のプロファイルを割り当てない場合、そのゾーン内の SonicPoint/SonicWave はリストの最初のプロファイルを使用します。

4 無線ゾーンにインターフェースを割り当てます。

5 無線ゾーン内のインターフェースに アクセス ポイント を接続します。

6 アクセス ポイントをテストします。

SonicPoint/SonicWave ファームウェアの更新

すべての SonicOS ファームウェアに SonicPoint/SonicWave ファームウェアのイメージが含まれるわけではありません。「**接続 | アクセス ポイント>基本設定**」ページの最上部を確認して、「**ダウンロード**」リンクを探します。

SonicWall 装置がインターネットに接続できる場合は、SonicPoint/SonicWave 機器を接続したときにファイアウォール サーバから SonicPoint/SonicWave イメージの最新バージョンが自動的にダウンロードされます。

SonicWall 装置がインターネットにアクセス *できない*か、プロキシ サーバを通じてのみアクセスできる場合は、SonicPoint/SonicWave イメージを更新する必要があります。

SonicPoint/SonicWave ファームウェアを手動で更新するには、以下の手順に従います。

1 http://www.mysonicwall.com からインターネットにアクセスできるローカル システムに SonicPoint/SonicWave イメージをダウンロードします。

SonicPoint/SonicWave イメージは次の場所からダウンロードできます。

- SonicOS ファームウェアをダウンロードできるのと同じページ
- 「ダウンロード センター」ページ (「**種別**」ドロップダウン メニューの「**SonicPoint/SonicWave**」を選択)

2 SonicWall 装置から到達できるローカル ウェブ サーバに SonicPoint/SonicWave イメージをロードします。

SonicPoint/SonicWave イメージのファイル名は変更してもかまいませんが、拡張子はそのままにしておいてください (例えば、`.bin.sig`)。

3 SonicWall 装置のSonicOS ユーザ インターフェースで、「**管理 | システム セットアップ | 装置 > 基本設定**」に移動します。

4 「**システム セットアップ | 装置 > 基本設定**」ページの「**ダウンロード URL**」セクションで、ダウンロードする SonicPoint/SonicWave イメージに対応するチェックボックスをオンにします (複数のイメージをダウンロードできます)。

- **SonicPoint-N イメージ URL を手動で指定 (http://)**
- **手動で SonicPoint-Ni/Ne のイメージの URL を指定する (http://)**
- **SonicPoint-NDR イメージの URL を手動で指定する (http://)**
- **SonicPoint-ACe/ACi/N2 イメージ URL(http://) を手動で指定**
- **SonicWave 432o/e/i イメージ URL (http://) を手動で指定**

5 上記のフィールドに、ローカル ウェブ サーバ上の SonicPoint/SonicWave イメージ ファイルの URL を入力します。

メモ：SonicPoint/SonicWave イメージ ファイルの URL を入力する際、"http://" の部分はフィールドに入力しないでください。

6 「**適用**」を選択します。

SonicPoint/SonicWave をリセットする

SonicPoint および SonicWave 432 e/i のリセット スイッチは、背面のコンソール ポートの隣の小さな穴の中にあります。伸ばしたクリップや楊枝のような細くてまっすぐなものでこのリセット スイッチを押すと、アクセス ポイントをいつでもリセットできます。

メモ：SonicWave 432o にはリセット ボタンは搭載されていません。

リセット ボタンを押すと、アクセス ポイントの動作中のモードの設定が、工場出荷時の設定に戻ります。他方のモードの設定はリセットされません。アクセス ポイントの動作中のモード、およびリセット ボタンを押す時間の長さに応じて、アクセス ポイントの動作は次のいずれかになります。

- 管理モードで動作中のでリセット ボタンを **3 秒以上、8 秒未満押すと、**管理モードの設定が工場出荷時の設定に戻り、アクセス ポイントが再起動されます。
- 管理モードで動作中のアクセス ポイントでリセット ボタンを **8 秒より長く**押すと、管理モードの設定が工場出荷時の設定に戻り、アクセス ポイントがセーフモードで再起動されます。
- リセット ボタンを **3 秒以上**押すと、設定が工場出荷時の設定に戻り、アクセス ポイントが再起動されます。

アクセス ポイントと RADIUS アカウント

メモ：RADIUS を使用したユーザ認証については、「RADIUS サーバの設定」を参照してください。

RADIUS (リモート認証ダイヤルイン ユーザ サービス) は、認証、承認、アカウンティングの一元化を実現するネットワーク プロトコルです。SonicOS では RADIUS プロトコルを使用して、NAS (ネットワーク アクセス サーバ、この場合はアクセス ポイント) から RADIUS アカウント サーバにアカウント情報を配信します。このアカウント情報は、RADIUS アカウント サーバ側でさまざまな課金ルールを適用するために利用できます。このアカウント情報は、ユーザごとのセッション時間や転送中のトラフィック負荷に基づいたものにすることができます。

全体的な認証、承認、アカウンティングの処理は、次のように機能します。

1 ユーザと SonicWall ファイアウォールに接続されているアクセス ポイントとの関連が生じます。
2 指定されている方式を使用して認証が実行されます。
3 IP サブネット/VLAN 割り当てが有効になります。
4 アクセス ポイントが RADIUS アカウント要求開始メッセージをアカウント サーバに送信します。
5 必要に応じて再認証が実行されます。
6 再認証の結果に基づき、アクセス ポイントが暫定的なアカウント更新情報をアカウント サーバに送信します。

7 ユーザとアクセス ポイントとの関連がなくなります。

アクセス ポイントが RADIUS アカウント要求停止メッセージをアカウント サーバに送信します。

RADIUS アカウント サーバの設定

RADIUS アカウント サーバを設定するには、以下の手順に従います。

1 次のように RADIUS クライアントのエントリを `/etc/freeradius/clients.conf` ファイルに追加します。

```
Client <IP アドレス> {
     Secret = "<パスワード>"
}
```

ここで、*<IP アドレス>* は RADIUS サーバの IP アドレスであり、*<パスワード>* はサーバのパスワードです。

メモ：IP アドレスは、RADIUS サーバに到達できる SonicWall GW の WAN IP です。

2 次のようにユーザ情報を `/etc/freeradius/users` ファイルに追加します。

```
ユーザ名 Cleartext-Password := "<パスワード>"
```

ここで、*ユーザ名* はユーザの ID であり、*<パスワード>* はユーザのパスワードで置き換える必要があります。

3 freeradius を開始するには、コマンド

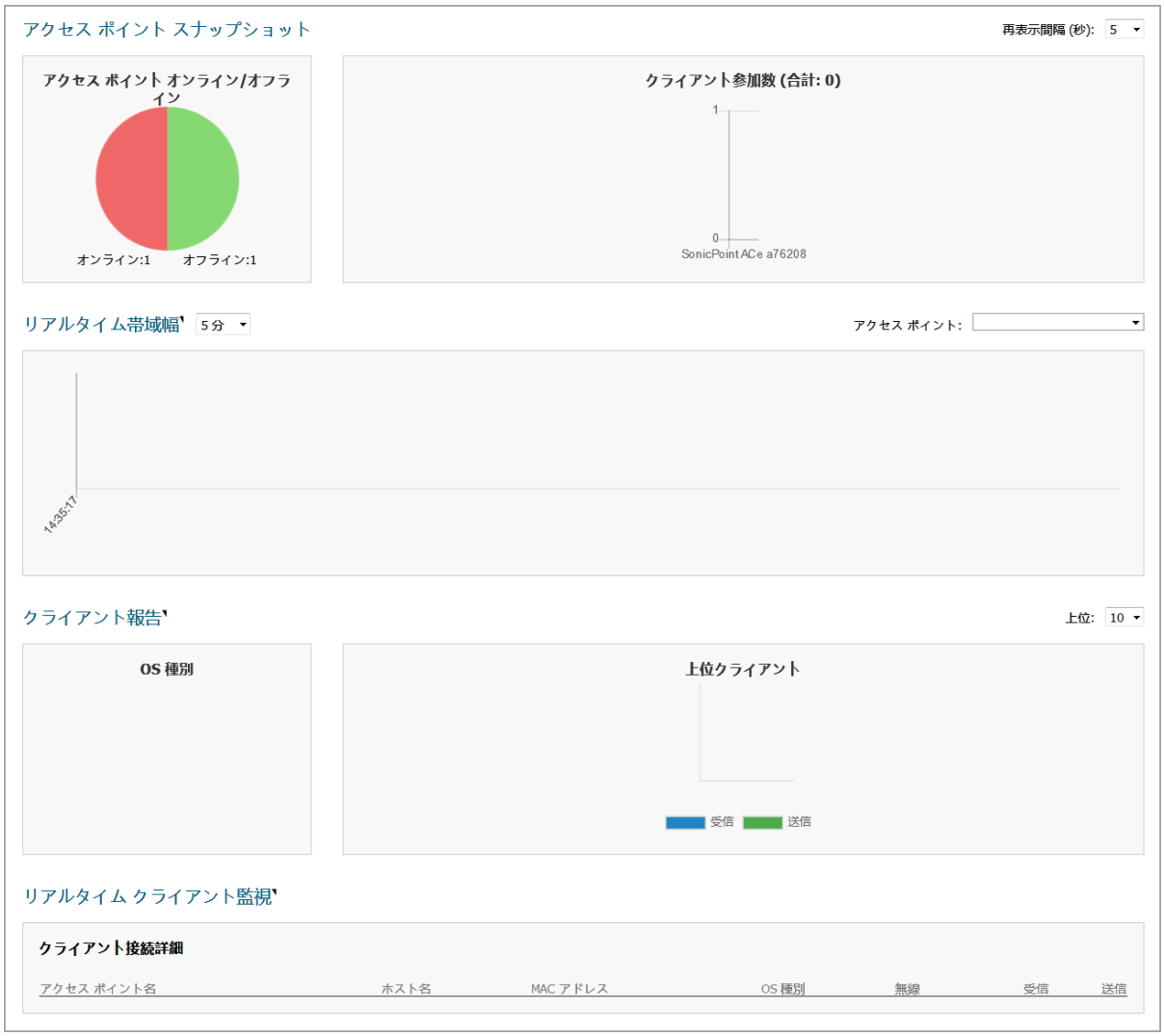
```
sudo feeradius -X
```

をコマンド ラインから実行します。

15

アクセス ポイント ダッシュボード

SonicWave および SonicPoint AC 機器に対して、**接続 | アクセス ポイント > ダッシュボード** は、表やグラフを使ってインフラの一部であるアクセス ポイントに関連したデータを視覚化します。リアルタイムの状態および状態の履歴を両方とも表示できるほか、個別のクライアントの速度、OS の種類およびホスト名も表示します。また、SonicWave および SonicPoint 機器の状態も表示し、さらに監視と問題の診断を支援する情報も提供します。



メモ：一部のバージョンの SonicOS 6.5で、ダッシュボードの体裁が異なる場合があります。詳細については、以下のトピックのダッシュボード ページ セクションの説明を参照してください。

トピック:

機能上の制限

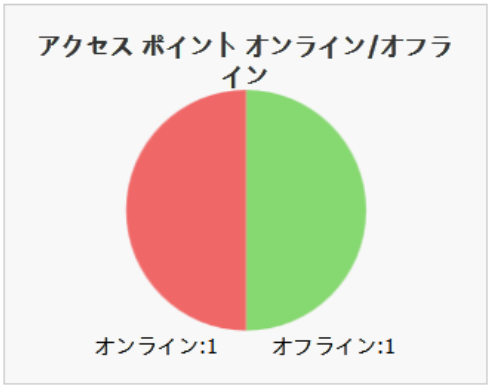
SonicWave および SonicPoint AC 機器の状態は、機器が SonicWallファイアウォールによって管理されている場合に表示されます。ファイアウォールと アクセス ポイント の両方が機能している必要があります。そうでない場合、有効なデータが交換されません。SonicWave アクセス ポイントは、常時、ダッシュボード データの 7 日間の履歴を保持します。ただし、メモリの制限により、SonicPoint AC 機器は再起動されるとすべての履歴データを失います。

アクセス ポイント スナップショット

「接続 | アクセス ポイント> ダッシュボード」の**「アクセス ポイント スナップショット」**セクションには、2 つのグラフが表示されます。**「アクセス ポイント オンライン/オフライン」**と**「クライアント参加数」**です。右の方で、これらの表を更新する間隔を指定できます。ドロップダウン メニューから分数を選択してください。オプション範囲は 5〜10 分です。

アクセス ポイント オンライン/オフライン

「アクセス ポイント オンライン/オフライン」グラフは、インフラ内のアクセス ポイントの状態を短くまとめて表示します。データは円グラフで表示されます。オンラインは緑色、オフラインは赤色です。グラフの下には、アクセス ポイントの数と状態が表で表示されます。

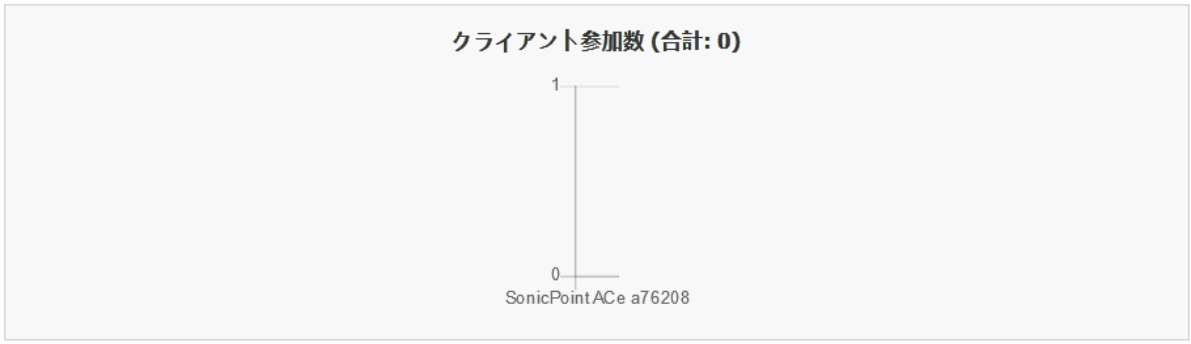


オンライン ステータスには、動作中、無効、再起動中、IDS スキャン モードが含まれます。

オフライン ステータスには、無応答および初期化状態が含まれます。

クライアント参加

「**クライアント参加**」グラフは、構成内の個別のアクセス ポイントに関連付けられたクライアントの数を表示します。ユーザ数は棒グラフ形式で表示されます。

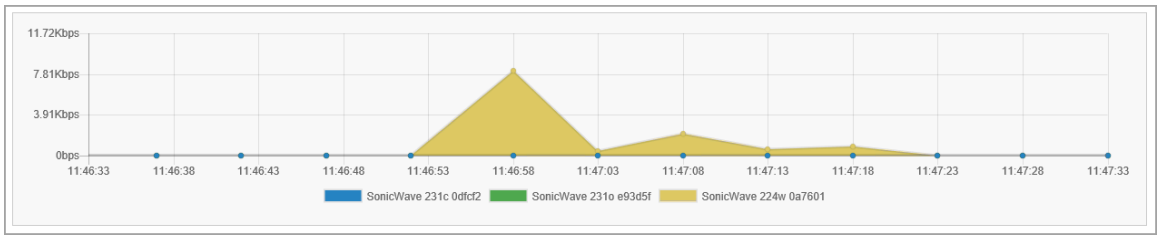


リアルタイム帯域幅

「**接続 | アクセス ポイント> ダッシュボード**」の「**リアルタイム帯域幅** 」セクションには、選択されたアクセス ポイントで使用されている帯域幅のグラフが表示されます。

メモ：SonicPoint ACe/ACi/N2 および SonicWave 機器だけが、「**リアルタイム帯域幅**」機能をサポートしています。

SonicOS は、選択したアクセス ポイント のリアルタイム トラフィックの積み上げグラフを示します。Y 値は、受信および送信の両方の合計トラフィックです。既定では、すべての アクセス ポイント が表示用に選択されています。



更新間隔を選択するには、グラフのタイトルの近くにあるドロップダウン メニューから更新間隔を選択してください。オプションは以下のとおりです。**1 分**、**2 分**、**5 分**、**10 分**、**60 分** です。

表示するアクセス ポイントを変更するには、「**アクセス ポイント**」ドロップダウン メニューに移動して、別の機器を選択してください。グラフは、当該の アクセス ポイント に対するデータに更新されます。

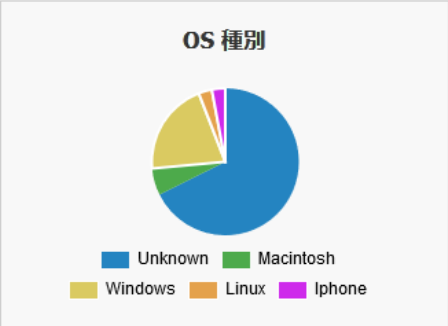
クライアント報告

「接続 | アクセス ポイント> ダッシュボード」の**「クライアント報告」**セクションには、2 つのグラフが表示されます。**「OS 種別」**と**「上位クライアント」**です。

メモ：クライアント レポート機能をサポートするのは、SonicPoint ACe / ACi / N2 および SonicWave 機器のみです。

OS 種別

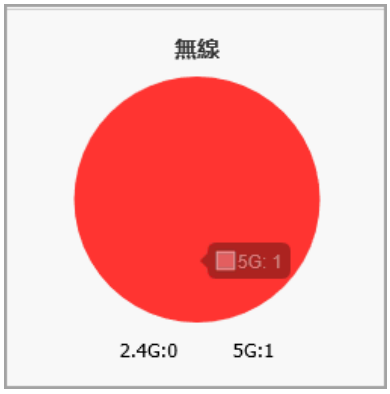
OS 種別円グラフには、接続されている Windows クライアント、Macintosh クライアント、Linux クライアント、iPhone、Android などの割合が表示されます。クライアントが HTTP トラフィックを生成していない場合、「*不明*」と表示されることがあります。



メモ：OS 種別機能をサポートするのは、SonicPoint ACe / ACi / N2 および SonicWave 機器のみです。

無線

SonicOS 6.5.2 以降では、**クライアント レポート**は**無線**チャートも提供します。**無線**チャートには、2.4GHz 無線と 5GHz 無線に接続されているクライアントの割合が表示されます。



メモ：無線機能をサポートするのは、SonicPoint ACe / ACi / N2 および SonicWave 機器のみです。

上位クライアント

「**上位クライアント**」グラフは、誰が一番帯域幅を使用しているかを表示します。「**上位**」フィールドに移動してドロップダウン メニューから数を選択します。帯域幅使用者のトップ 5、トップ 10、トップ 15、またはトップ 20 を表示できます。上位ユーザについて、送信および受信データの数値が表示されます。

メモ：上位クライアント機能をサポートするのは、SonicPoint ACe / ACi / N2 および SonicWave 機器のみです。

リアルタイム クライアント監視

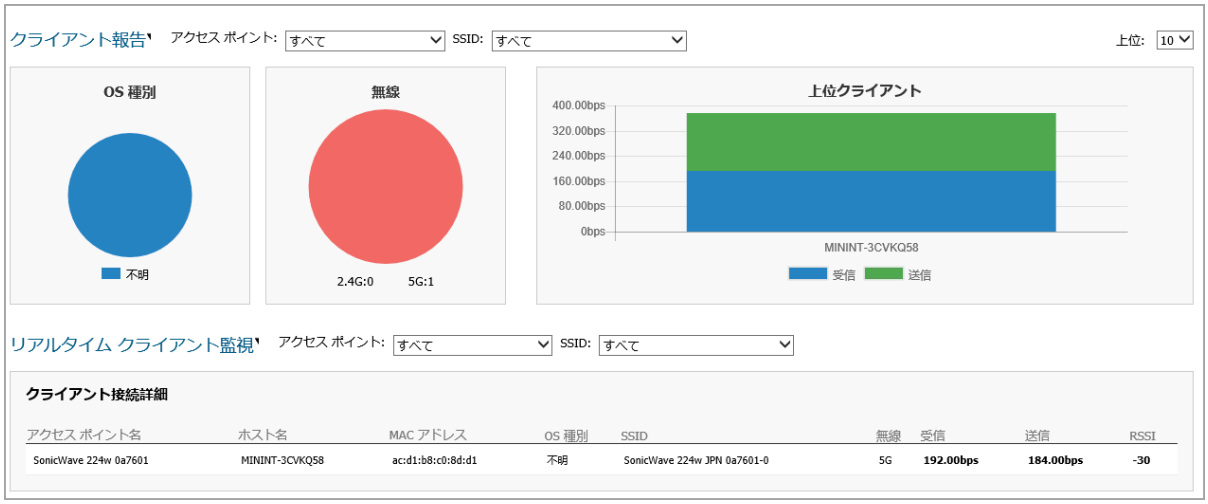
「**接続 | アクセス ポイント> ダッシュボード**」の「**リアルタイム クライアント監視**」セクションには、クライアント接続状況の詳細グラフが表示されます。アクセス ポイントを通じて接続している個別のユーザの詳細を提供します。MAC アドレス、OS 種別、受信 (Rx) トラフィック量、および送信 (Tx) トラフィック量が表示できます。

メモ：SonicPoint ACe/ACi/N2 および SonicWave 機器だけが、**リアルタイム クライアント監視**機能をサポートしています。

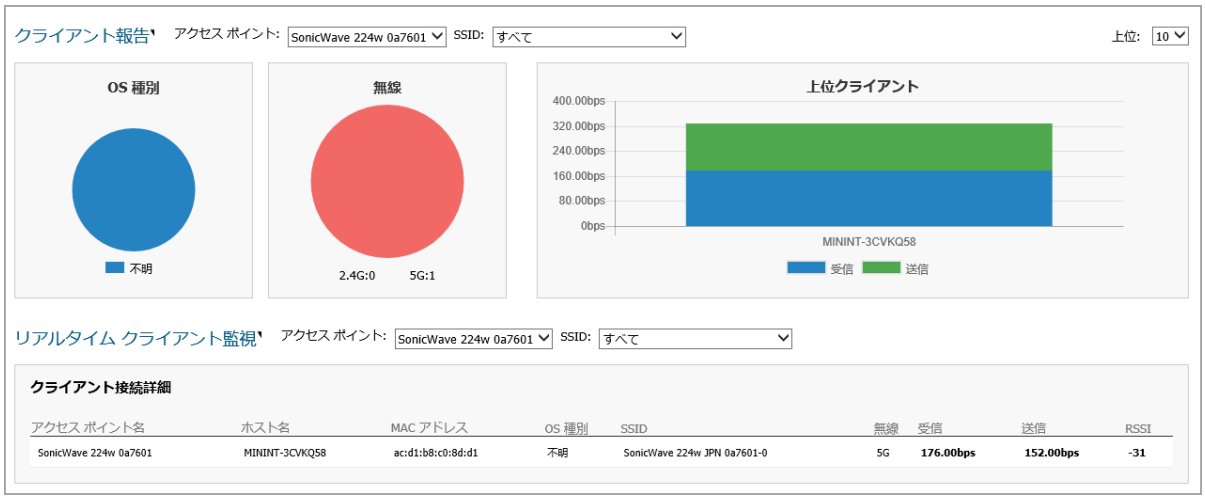
クライアント報告とクライアント監視フィルタリング

SonicOS 6.5.2 以降から、「**クライアント報告**」セクションと「**リアルタイム クライアント監視**」セクションの両方で出力をフィルタリングできます。具体的には、「*すべて*」または特定の アクセス ポイント を「**アクセス ポイント**」ドロップダウン メニューで選択します。または「*すべて*」または特定の SSID を「**SSID**」ドロップダウン メニューで選択します。

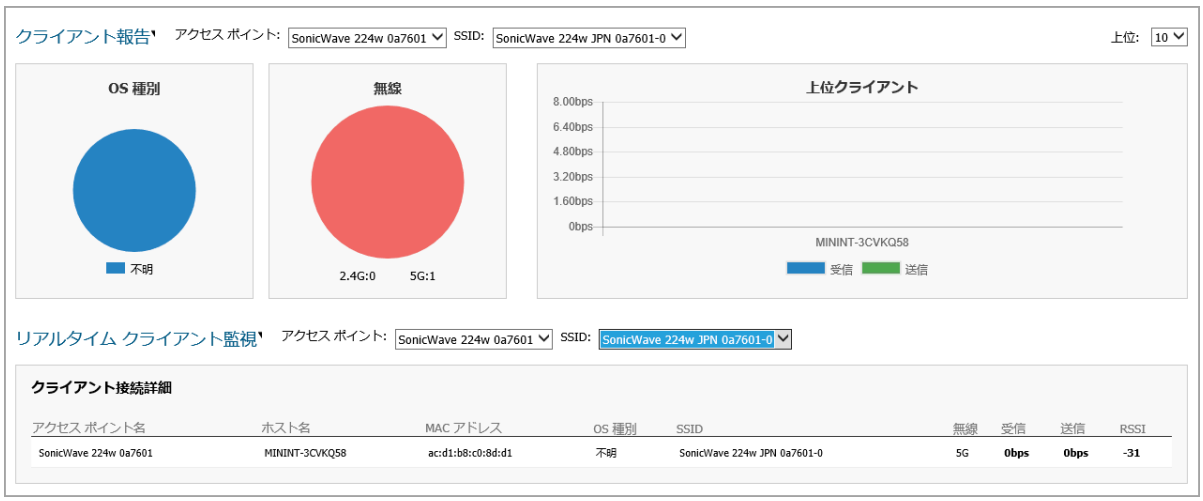
すべてのクライアントの詳細



アクセス ポイントでフィルタリングされたクライアントの詳細



アクセス ポイントと SSID でフィルタリングされたクライアントの詳細



メモ：SonicPoint ACe / ACi / N2 および SonicWave 機器のみがクライアント詳細フィルタリングをサポートします。

16

アクセス ポイント基本設定

無線アクセス ポイントをプロビジョニングするうえで最も効率的な方法は、SonicOS ファイアウォールに自動的にアクセス ポイントを検出させて、既定プロファイルのうちの 1 つを使用することです。SonicOS には、SonicWall アクセス ポイント の各世代に合わせて 1 つずつ、合計 4 つの既定プロファイルが提供されています。具体的には SonicPointN、SonicPointNDR、SonicPointACe/ACi/N2、および SonicWave です。これらはそのまま使用することも、設定に合わせてカスタマイズすることもできます。SonicWall アクセス ポイント の種類に基づいて、新規のプロファイルを作ることもできます。

「**管理 | 接続性 | アクセス ポイント > 基本設定**」ページの最上部には、情報メッセージが表示され、動作中のアクセス ポイントのファームウェア バージョンが示されます。「**同期**」ボタンはメッセージの下にあります。

アクセス ポイント プロファイルは、「**SonicPoint / SonicWave プロビジョニング プロファイル**」セクションに表示されます。各プロファイルを編集するか、新しいプロファイルを追加できます。

「**SonicPoint / SonicWave オブジェクト**」セクションには、接続されたアクセス ポイントの設定が表示されます。また、それらを編集したりその他のアクションを実行したりするための設定ボタンがあります。

メモ：無線 LAN を無効にすると、すべてのアクセス ポイントとワイヤレス関連のページが消えます。ゾーン種別から無線ゾーンが削除されます。また、既存の WLAN ゾーンやオブジェクトを一切編集できなくなります。

トピック:

- アクセス ポイントの同期
- プロビジョニングの概要
- プロビジョニング プロファイルの作成/変更
- アクセス ポイントの管理

アクセス ポイントの同期

「**接続 | アクセス ポイント > 基本設定**」ページの上部にある「**アクセス ポイントの同期**」をクリックして、 SonicWall 装置から WLAN ゾーンへクエリを発行します。接続されているすべてのアクセス ポイントが、それぞれの現在の設定と統計を装置に報告します。同時に SonicOS は、新規に接続されてファイアウォールにまだ登録されていないアクセス ポイントの存在を特定しようと試みます。

メモ：このボタンを選択すると、すべてのアクセス ポイントに対してポーリングが行われますが、それらに設定がプッシュされることはありません。

プロビジョニングの概要

SonicPoint/SonicWave で使用するプロファイルは、分散無線手法で複数の アクセス ポイント の設定と設定の配布を行うスケーラブルで高度に自動化された方法を提供します。SonicPoint/SonicWave プロファイルの定義には、2.4GHz および 5GHz の無線設定、SSID、動作チャンネルなど、SonicWall アクセス ポイント で設定できるすべての設定が含まれます。

アクセス ポイント プロファイルを定義し終えたら、そのプロファイルを無線ゾーンに適用することができます。各無線ゾーンを、それぞれ 1 つの アクセス ポイント プロファイルで設定することができます。1 つのプロファイルを任意の数のゾーンに適用することもできます。その後、アクセス ポイント がゾーンに接続すると、そのゾーンに割り当てられたプロファイルによって自動的にプロビジョニングされます。

アクセス ポイント 装置を最初に接続して電源を入れたとき、装置は工場出荷時の既定の設定が割り当てられます (IP アドレス `192.168.1.20`、ユーザ名: `admin`、パスワード: `admin`) として SonicWall 管理インターフェースにログインします。そして初期化中、通信相手となる SonicOS 機器を探します。SonicOS 機器が起動したとき、SonicWall 発見プロトコルを通じてアクセス ポイントを検知しようとします。アクセス ポイント および相手先 SonicOS 機器が相互に検出された場合は、その 2 つの装置間で暗号化された交換が発生し、関連する無線ゾーンに割り当てられたプロファイルを使用して、新たに追加された アクセス ポイント 装置が自動的にプロビジョニングされます。

プロビジョニング手順の一環として、SonicOS は検出された アクセス ポイント 機器に一意の名前を割り当て、MAC アドレスと、検出されたインターフェースおよびゾーンを記録します。また、IP アドレスを自動的に割り当てることもできます。このように設定しておけば、アクセス ポイント は認証サーバと通信して WPA-EAP をサポートすることができます。SonicOS は、該当するゾーンに関連付けられたプロファイルを使用して、2.4GHz および 5GHz の無線を設定します。

プロファイルに変更を行っても、すでにプロビジョニングされて動作状態にある装置には影響しません。動作している アクセス ポイント 機器に対して設定変更を行う方法は 2 とおりあります。

- 手動設定変更による方法

  単一または小規模な変更を行う場合に適しています。とりわけ、個々の アクセス ポイント で、そのゾーンに割り当てられたプロファイルとは異なる設定が必要なときに適した方法です。

- プロビジョニング取消による方法

  アクセス ポイントを削除することにより、その装置に対するプロビジョニングが有効に取り消されます。当該装置の設定はクリアされ、相手の SonicOS 機器との間で新規にプロビジョニング手順が自動的に行われる状態になります。この方法はゾーンのプロファイルを更新または変更し、その変更内容を伝播するように設定する場合に便利です。アクセス ポイント のファームウェアを更新したり、単に複数の アクセス ポイント 装置を一定の *制御された* やり方で自動的に更新したりするときに、この方法が使用できます。すべての アクセス ポイント を一度に変更すると、サービスに混乱が生じる可能性があるためです。

プロビジョニング プロファイルの作成/変更

「**管理**」表示の「**接続 | アクセス ポイント>基本設定**」で、個別の対象だけでなく、プロビジョニング プロファイルの設定と管理を行うことができます。任意の数のプロファイルを追加することができます。

メモ：*SonicPoint AC* は SonicPoint ACe/ACi/N2 を参照します。*SonicPoint* はすべての SonicPoint 機器を参照します。*SonicWave* は SonicWave 432e/i/o を参照します。SonicPoint AC は、SonicOS 6.2.2 以降を搭載する装置でサポート されています。SonicWave 機器は、SonicOS 6.5 以降でサポート されています。

「**接続 | アクセス ポイント>基本設定**」ページに移動します。「**SonicPoint/SonicWave プロビジョニング プロファイル**」セクションに、4 つの既定 SonicOS プロファイルと共に、作成した個別プロファイルが表示されます。既定のプロビジョニング プロファイルを変更する場合、「設定」アイコンを選択し、適切な変更を行ってください。

重要：**SonicPoint/SonicWave プロビジョニング プロファイル** の作成または変更はすべての種類のアクセス ポイントを通じて同様であるため、このセクションでは SonicWave 機器に対して新規プロファイルを追加する方法を確認します。一般的な手順に対して重大な違いがある場合には注記して、このセクションの後の方で詳細を説明します。

メモ：SonicWall が提供するプロビジョニング プロファイルは削除することができません。したがって、該当する「**削除**」アイコンはグレーアウトされて無効になっています。

「**新規プロファイルの追加**」オプションには、類似の設定をグループ化した複数の画面があります。手順は、それらの画面に合わせてグループ化されています。

トピック:

プロビジョニング プロファイルの追加/編集 - はじめに

新しいプロファイルを追加するには:

1 「**管理**」表示で、「**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**」セクションの「**新規プロファイルの追加**」フィールドで、作成したいプロファイルの種類を選択します。この例では、**SonicWave プロファイル**が選択されています。

メモ：既存のプロファイルを変更するには、更新したいプロファイルの「**設定**」アイコンを選択します。

プロビジョニング プロファイルの一般設定

「一般」画面でオプションを設定するには:

1 「**SonicWave 設定**」を設定します。

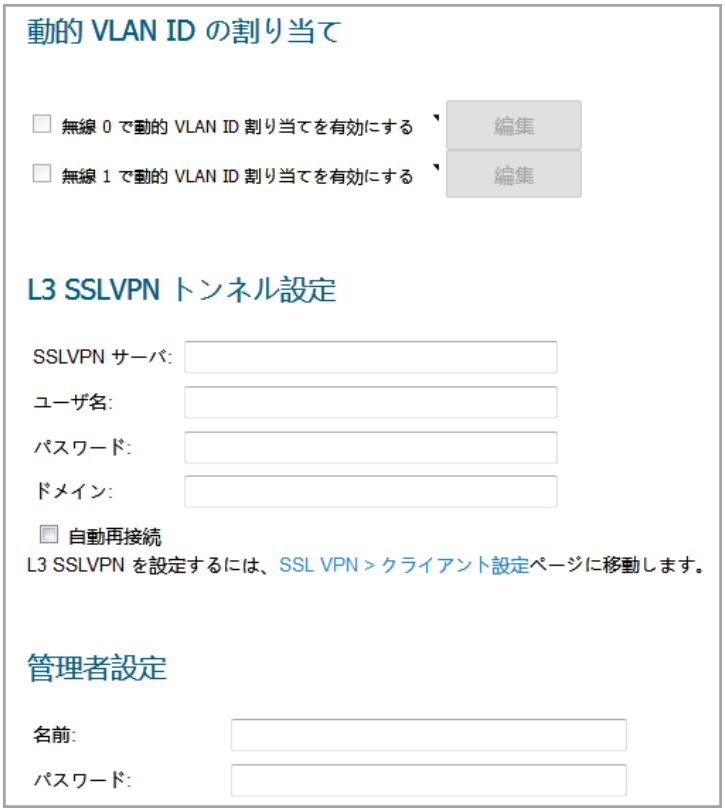
オプション	動作
SonicWave を有効にする	このチェックボックスにチェックを入れると、SonicWave アクセス ポイント が有効になります。これは既定でオンになっています。
設定を保持	このチェックボックスにチェックを入れると、カスタマイズした設定を装置が次に再起動されるまで保持します。「**編集**」ボタンが有効になっていれば、「**設定を保持**」ダイアログが開くので、どの設定を保持するかをカスタマイズできます。 
RF 監視を有効にする	このチェックボックスにチェックを入れると、無線 RF 脅威のリアルタイム監視と管理が有効になります。
LED を有効にする	このチェックボックスにチェックを入れると、SonicWave LED が有効になります。このチェックボックスにチェックを入れないまま (既定値) にしておくと、LED は無効のままになります。
低電力モードを有効にする	このチェックボックスにチェックを入れると、SonicWave が低電力モードで動作することを許可します。電源が標準の 802.3at PoE ではない場合に使用します。
名前開始文字列	名前の先頭部分で使用する文字列を所定のフィールドに入力します。
国番号	ドロップダウン メニューから、アクセス ポイントを配備する国の国番号を選択します。
EAPOL バージョン	ドロップダウン メニューから EAPoL バージョンを選択します。V2 の方がセキュリティが向上することに注意してください。
帯域誘導モード	ドロップダウン メニューから帯域誘導モードを選択します。オプションは以下を含みます。**無効**、**自動**、**5GHz を優先**、または **5GHz を強制**。

2 **仮想アクセス ポイント設定**を設定するには、以下の手順に従います。

a 「**5GHz 無線仮想 AP グループ**」で、ドロップダウン メニューから仮想アクセス ポイント オブジェクト グループを選択します。

b 「**2.4GHz 無線仮想 AP グループ**」で、ドロップダウン メニューから仮想アクセス ポイント オブジェクト グループを選択します。

3 **一般設定**が見えるまで下にスクロールします。



4 「**動的 VLAN ID の割り当て**」を設定します。

> **メモ：動的 VLAN ID 割り当て**の下のオプションを有効にするには、WLAN ゾーンと VLAN インターフェースを**システム セットアップ | ネットワーク**で作成する必要があります。

5 **SSL VPN トンネル設定**の構成

a テキスト フィールドに **SSL VPN サーバ**名または IP アドレスを入力します。

b SSL VPN サーバ用の **ユーザ名** をフィールドに入力します。

c SSL VPN サーバ認証用の **パスワード** を入力します。

d **ドメイン** 名をフィールドに入力します。

e **自動再接続** の有効化チェックボックスをオンにします。

f レイヤ 3 SSL VPN を設定する場合、「**接続 | SSL VPN > クライアントの設定**」へのリンクをたどって、適切な設定を定義してください。

6 「**管理者設定**」を設定します。

a ネットワーク管理者の**ユーザ名**を入力します。

b ネットワーク管理者の**パスワード**を入力します。

プロビジョニング プロファイルの 5GHz/2.4GHz 無線の基本設定

さまざまなアクセス ポイントで、5GHz 無線と 2.4GHz 無線の基本設定は似ており、わずかな違いしかありません。相違点については、手順の中で示します。

以下のトピックでは、「**5GHz/2.4GHz 無線の基本**」画面の設定について説明します。

- 無線設定
- 無線セキュリティ
- 保護された管理フレーム (PMF オプション)
- ローカル RADIUS サーバと EAP 認証バランスについて
- RADIUS サーバの設定
- ACL 強制
- リモート MAC アドレス アクセス制御の設定

無線設定

5GHz 無線/2.4GHz 無線の基本設定を行うには:

1 「**5GHz 無線の基本**」または「**2.4GHz 無線の基本**」を選択します。

2 「**無線を有効にする**」をオンにすると、このプロファイルでプロビジョニングされたすべてのアクセス ポイント で無線帯域が自動的に有効になります。このオプションは、既定では選択されています。

3 「**無線を有効にする**」ドロップダウン メニューで、無線をオンにする時間のスケジュールを選択するか、新しいスケジュールを作成します。既定は「**常に有効**」です。

4 「**モード**」ドロップダウン メニューから適切な無線モードを選択します。

無線モードの選択肢

5GHz 無線の基本	2.4GHz 無線の基本	定義
5GHz 802.11n のみ	2.4GHz 802.11n のみ	802.11n クライアントだけが無線ネットワークにアクセスできます。この制限付き無線機モードでは、802.11a/b/g クライアントは接続できません。
5GHz 802.11n/a 混在	2.4GHz 802.11n/g/b 混在 (SonicPoint AC/NDR 既定値)	802.11a および 802.11n (5GHz 無線) または 802.11b、802.11g、および 802.11n (2.4GHz 無線) のクライアントを同時にサポートします。無線ネットワークが複数の種類のクライアントで構成されている場合は、このモードを選択してください。
5GHz 802.11a のみ (SonicPoint NDR 既定値)		802.11a クライアントだけが無線ネットワークにアクセスする場合は、このモードを選択します。
	2.4GHz 802.11g のみ	無線ネットワークが 802.11g クライアントだけで構成されている場合は、802.11g パフォーマンスを向上させるためにこのモードの選択をお勧めします。このモードを選択すると、802.11b クライアントの参加を防ぐこともできます。
5GHz 802.11ac/n/a 混在 (SonicWave と SonicPoint AC 既定値)		802.11ac、802.11a、および 802.11n のクライアントを同時にサポートします。無線ネットワークが複数の種類のクライアントで構成されている場合は、このモードを選択してください。
5GHz 802.11ac のみ		802.11ac クライアントだけが無線ネットワークにアクセスできます。この制限付き無線モードでは、他のクライアントは接続できません。

ヒント：802.11n クライアントのみ802.11n クライアントだけを対象に最適なスループット速度を実現するには、「**802.11n のみ**」無線モードをお勧めします。複数の無線クライアント認証の互換性を維持するには、「**802.11n/g/b 混在**」無線モードを使用してください。

802.11ac クライアントだけを対象に最適なスループット速度を実現するには、「**802.11ac のみ**」無線モードをお勧めします。「**802.11ac/n/a 混在**」無線モードは、複数無線クライアント認証互換性の用途で使用します。

メモ：「**802.11n 5GHz/2.4GHz 無線設定**」で使用可能なオプションは、選択したモードによって変わります。無線の設定モードによって、以下のようになります。

- 802.11n をサポートするモードの場合は、「**無線帯域**」、「**プライマリ チャンネル**」、「**セカンダリ チャンネル**」、「**ショート ガード間隔を有効にする**」、「**凝集 (アグリゲーション) を有効にする**」のオプションが表示されます。
- 802.11n をサポートしないモードの場合は、「**チャンネル**」オプションのみが表示されます。

5 「**SSID**」フィールドに、このプロファイルを使用する各 アクセス ポイント の SSID として認識可能な文字列を入力します。これが、利用可能な無線接続のクライアント一覧に表示される名前になります。

ヒント：組織内のすべての SonicPoint または SonicWaves で同じ SSID を共有していれば、ユーザが アクセス ポイント間でローミングを行うときに無線接続の維持が容易になります。

6 それ以外のモードの場合は、「**無線帯域**」ドロップダウン メニューから無線帯域を選択します。

メモ：「**モード** = **5GHz 802.11a のみ**」の場合、**無線帯域**オプションは利用不可です。

- 「**自動**」- 装置は信号の強度と整合性に基づいて、無線動作に最適なチャンネルを自動的に検出および設定できます。 1 つが選択された場合、「**プライマリ チャンネル**」と「**セカンダリ チャンネル**」も「**自動**」に設定しなくてはなりません。このオプションは既定の設定です。
- 「**標準 - 20MHz チャンネル**」- 無線が標準 20MHz チャンネルのみを使用するように指定します。
- 「**広域 - 40 MHz チャンネル**」- **5GHz 802.11a のみ** が **無線帯域** で選択されている場合を除いて、すべてのモードで利用可能です。無線が広域 40MHz チャンネルのみを使用するように指定します。
- 「**広域 - 80 MHz チャンネル**」-「**5GHz 802.11ac/n/a 混在**」または「**5GHz 802.11ac のみ**」が「**無線帯域**」として選択されている場合のみ利用可能で、5GHz 無線 が広域 80MHz チャンネルのみを使用するように指定します。(「**モード**」が「**5GHz 802.11n のみ**」、「**5GHz 802.11n/a 混在**」、または「**5GHz 802.11a のみ**」のときは使用できません。)

7 チャンネルを、**モード**および**無線帯域**オプションの選択に合わせて選択してください。

モード	無線帯域	チャンネル
5GHz 802.11n のみ	自動	「**プライマリ チャンネル**」と「**セカンダリ チャンネル**」フィールドの既定値は**自動**です。
	標準 - 20 MHz チャンネル	「**自動**」または「**標準チャンネル**」ドロップダウン メニューで指定された無線チャンネルの 1 つを選択します。
	広域 - 40 MHz チャンネル	「**自動**」または「**プライマリ チャンネル**」の無線チャンネルの 1 つを選択します。「**セカンダリ チャンネル**」は自動的に「**自動**」に定義されます。
5GHz 802.11n/a 混在	自動	「**プライマリ チャンネル**」と「**セカンダリ チャンネル**」フィールドの既定値は**自動**です。
	標準 - 20 MHz チャンネル	「**自動**」または「**標準チャンネル**」ドロップダウン メニューで指定された無線チャンネルの 1 つを選択します。
	広域 - 40 MHz チャンネル	「**自動**」または「**プライマリ チャンネル**」の無線チャンネルの 1 つを選択します。「**セカンダリ チャンネル**」は自動的に「**自動**」に定義されます。

モード	無線帯域	チャンネル
5GHz 802.11a のみ	(オプションはありません)	「**自動**」または「**チャンネル**」ドロップダウン メニューで指定された無線チャンネルの 1 つを選択します。
5GHz 802.11ac/n/a 混在	自動	「**チャンネル**」フィールドの既定値は**自動**です。
	標準 - 20 MHz チャンネル	「**自動**」または「**チャンネル**」ドロップダウン メニューで指定された無線チャンネルの 1 つを選択します。
	広域 - 40 MHz チャンネル	「**自動**」または「**チャンネル**」フィールドで指定された無線チャンネルの 1 つを選択します。
	広域 - 80 MHz チャンネル	「**自動**」または「**チャンネル**」フィールドで指定された無線チャンネルの 1 つを選択します。
5GHz 802.11ac のみ	自動	「**チャンネル**」フィールドの既定値は**自動**です。
	標準 - 20 MHz チャンネル	「**自動**」または「**チャンネル**」ドロップダウン メニューで指定された無線チャンネルの 1 つを選択します。
	広域 - 40 MHz チャンネル	「**自動**」または「**チャンネル**」フィールドで指定された無線チャンネルの 1 つを選択します。
	広域 - 80 MHz チャンネル	「**自動**」または「**チャンネル**」フィールドで指定された無線チャンネルの 1 つを選択します。

8 「**ショート ガード間隔を有効にする**」チェックボックスをオンにします。ガード間隔を短くすることによって、無線転送速度を上げます。無線クライアントもこれをサポートしていることを確認し、互換性の問題が発生しないようにしてください。

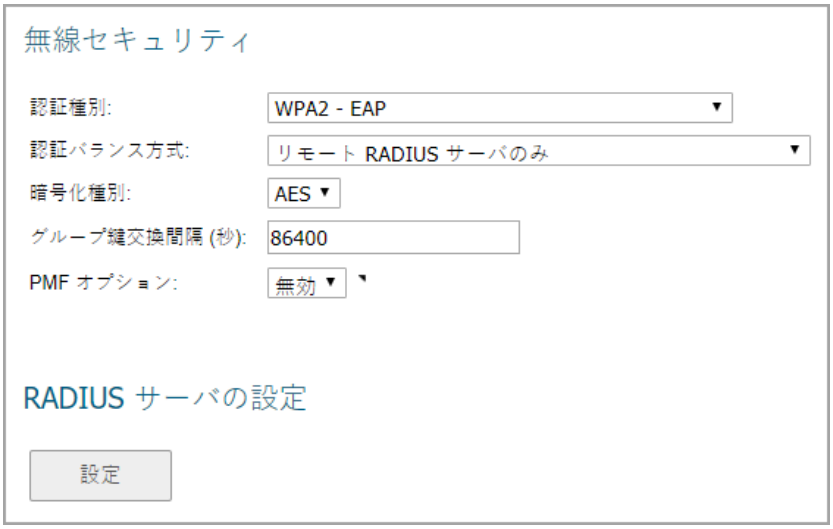
9 「**凝集 (アグリゲーション) を有効にする**」チェックボックスをオンにします。単一の伝送で複数のデータ フレームを送信することにより、無線スループットを上げます。無線クライアントもこれをサポートしていることを確認し、互換性の問題が発生しないようにしてください。

無線セキュリティ

メモ：SonicOS インターフェースは、文脈によって表示が変わります。「**一般**」画面で VAP グループが選択されている場合、「**無線セキュリティ**」セクションは飛ばせるように表示されません。

無線セキュリティ オプションを設定するには、以下の手順に従ってください。

1 **無線セキュリティ** セクションまでスクロールします。これらのオプションは、選択した**認証種別**によって変化します。



無線セキュリティを設定するには、以下の手順に従います。

1 「**無線セキュリティ**」セクションで、「**認証種別**」をドロップダウン メニューから選択します。

> **メモ**：使用可能なオプションは、選択した設定の種別によって変わります。**WPA2 - EAP** オプションが選択されている場合は、「**設定**」ボタンとともに「**RADIUS サーバ設定**」セクションが表示されます。

2 以下のテーブルを参考にして、残りの設定を定義します。

無線セキュリティのための WEP 設定

	WEP の説明	
認証種別	**WEP 鍵のモード**	**設定**
WEP (Wired Equivalent Privacy) は、Wi-Fi 無線ネットワーク セキュリティ用の規格です。公開システムで、認証のため情報を交換し、その後データを暗号化します。共有キーは事前共有鍵を使って認証します。		
WEP - 両方 (オープン システムと共有鍵)	**WEP 鍵モード** = **なし**	残りの設定はグレー表示になっていて選択できません。
	WEP 鍵モード = **64 ビット、128 ビット** または **152 ビット** ビット数が、WEP 鍵の強度を表します。	1 「**既定の鍵**」フィールドでは、既定値の鍵 (最初に試行した鍵) を選択してください。**第 1 鍵**が既定値です。 2 「**鍵登録**」フィールドでは、鍵を「**英数字**」とするか「**16 進数字 (0 ～ 9、A ～ F)**」とするか選択してください。 3 鍵 1、鍵 2、鍵 3、鍵 4 のフィールドに、データを転送する際に使用する暗号化鍵を入力します。
WEP - オープン システム		残りの設定はグレー表示になっていて選択できません。
WEP - 共有鍵	**WEP 鍵モード** = **64 ビット、128 ビット** または **152 ビット** 既定値は **152 ビット**です。	1 「**既定の鍵**」フィールドでは、既定値の鍵 (最初に試行した鍵) を選択してください。**第 1 鍵**が既定値です。 2 「**鍵登録**」フィールドでは、鍵を「**英数字**」とするか「**16 進数字 (0 ～ 9、A ～ F)**」とするか選択してください。**16 進数字**が既定値です。 3 鍵 1、鍵 2、鍵 3、鍵 4 のフィールドに、データを転送する際に使用する暗号化鍵を入力します。

WPA2 無線セキュリティ設定

認証種別	設定
	説明
WPA および WPA2 (Wi-Fi Protected Access) は、無線機器の保護のためのより新しいプロトコルです。「**WPA2 - 自動**」オプションの 1 つを選択しておくと、機器で WPA2 が有効になっていない場合には WPA プロトコルを使用します。	
WPA2 - PSK	1 ドロップダウン メニューから「**暗号化種別**」を選択します。オプションには、「**AES**」(既定)、「**TKIP**」、「**自動**」があります。 2 **グループ鍵交換間隔** を秒数で設定します。既定値は **86400** です。 3 SonicWave の場合、ドロップダウン メニューから「**PMF オプション**」を選択します。詳細については、「保護された管理フレーム (PMF オプション) (193 ページ)」を参照してください。 4 公開共有鍵の **パスフレーズ** を定義します。
WPA2 - EAP	1 SonicWave の場合、ドロップダウン メニューから「**認証バランス方式**」を選択します。詳細については、「ローカル RADIUS サーバと EAP 認証バランスについて (194 ページ)」を参照してください。 2 ドロップダウン メニューから「**暗号化種別**」を選択します。オプションには、「**AES**」(既定)、「**TKIP**」、「**自動**」があります。 3 **グループ鍵交換間隔** を秒数で設定します。既定値は **86400** です。 4 SonicWave の場合、ドロップダウン メニューから「**PMF オプション**」を選択します。詳細については、「保護された管理フレーム (PMF オプション) (193 ページ)」を参照してください。

WPA2 無線セキュリティ設定

	説明
認証種別	**設定**
WPA2 - Auto - PSK	1 ドロップダウン メニューから「**暗号化種別**」を選択します。オプションには、「**AES**」(既定)、「**TKIP**」、「**自動**」があります。 2 **グループ鍵交換間隔** を秒数で設定します。既定値は **86400** です。 3 SonicWave の場合、ドロップダウン メニューから「**PMF オプション**」を選択します。詳細については、「保護された管理フレーム (PMF オプション) (193 ページ)」を参照してください。 4 公開共有鍵の **パスフレーズ** を定義します。
WPA2 - Auto - EAP	1 SonicWave の場合、ドロップダウン メニューから「**認証バランス方式**」を選択します。詳細については、「ローカル RADIUS サーバと EAP 認証バランスについて (194 ページ)」を参照してください。 2 ドロップダウン メニューから「**暗号化種別**」を選択します。オプションには、「**AES**」(既定)、「**TKIP**」、「**自動**」があります。 3 **グループ鍵交換間隔** を秒数で設定します。既定値は **86400** です。 4 SonicWave の場合、ドロップダウン メニューから「**PMF オプション**」を選択します。詳細については、「保護された管理フレーム (PMF オプション) (193 ページ)」を参照してください。

保護された管理フレーム (PMF オプション)

「**認証種別**」の設定が **WPA2** オプションのいずれかであるとき、「**PMF オプション**」設定を使用できます。「**PMF オプション**」設定は、SonicOS 6.5.2 以降のSonicWave プロファイルでサポートされています。この機能は、無線管理フレームの保護のための IEEE 802.11 標準に対する IEEE 802.11w-2009 修正をサポートします。また、Protected Management Frames (PMF) 標準としても知られています。

「**無線セキュリティ**」の下にある「**PMF オプション**」ドロップダウン リストから、次の設定のいずれかを選択できます。

- **無効** - このサービスは有効化されません。クライアントは PMF なしで接続します。
- **有効** - このサービスは、無線クライアントではオプションです。クライアントは、クライアント設定に基づいて、PMF の有無にかかわらず接続できます。
- **必須** - クライアントは、PMF を有効化しないと接続できません。

802.11i 修正により ***データ*** フレームは保護されますが、認証、認証解除、関連付け、解離、ビーコン、プローブなどの管理フレームは、ネットワーク サービスのセッションを開始または破棄するために無線クライアントで使用されます。暗号化して機密性を高めることができるデータ 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が聞き取り、理解する必要があるため、オープンまたは暗号化されていない状態で送信する必要があります。これらのフレームは暗号化できませんが、攻撃から無線媒体を保護するために偽装防御を実施する必要があります。例えば、攻撃者がクライアントの MAC アドレスを取得すると、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できます。いずれの状況でも、クライアントはログオフされます。

802.11w 修正は、Protected Management Frames (PMF) サービスによって保護されている堅牢な ***管理*** フレームのセットに適用されます。不参加、認証解除、ロバスト アクションの各フレームがこの対象になります。802.11w は特定の管理フレームのみを保護し、アクセス ポイントとクライアント間の通信には影響しません。802.11w は、アクセス ポイントとクライアントの両方で 802.11w が有効化されているときだけ効果を持つことができます。

802.11w には次のメリットがあります。

機密性	ユニキャスト管理フレームを暗号化します: • データ フレームと同じ PTK を使用する • 前もって暗号化されていないフレーム ヘッダーを追加認証データ (AAD) で保護する • 拡張 AES-CCM でユニキャスト管理フレームを処理する • 独立した受信シーケンス カウンタ (RSC) でリプレイ攻撃を防御する
グループ アドレス指定フレーム保護	ブロードキャスト/マルチキャスト整合性プロトコル (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、リプレイ攻撃を防ぎ、ブロードキャスト/マルチキャスト攻撃のなりすましからクライアントを保護します。ブロード/マルチキャスト管理フレームの場合: • WPA 鍵ハンドシェイク中に受信した新しい Integrity Group Temporal Key (IGTK) を使用する • 新しいアルゴリズム: Broadcast Integrity Protocol (BIP) • 新しい情報要素: 管理 MIC IE でシーケンス番号 + 暗号化ハッシュ (AES128-CMAC ベース) を使用
接続保護	セキュリティアソシエーション (SA) クエリは、再参加要求のスプーフィングによってクライアントがオフラインにされることを防ぐことができます。

ローカル RADIUS サーバと EAP 認証バランスについて

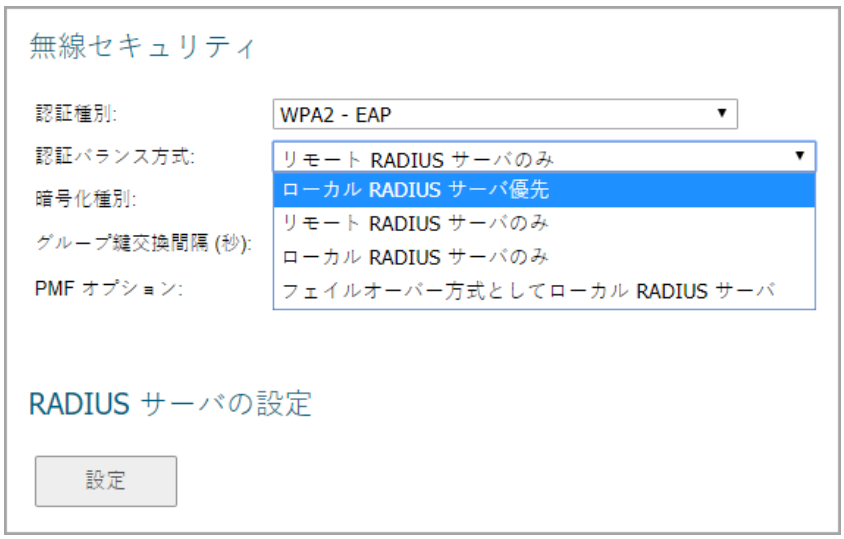
この機能は SonicOS6.5.2 で導入されました。これは、選択した SonicWave 内でローカル SonicWave アクセス ポイントがローカル RADIUS 認証サービスを提供できるようにします。また、ネイティブな LDAP システムや Active Directory を含む企業ディレクトリ サービスと統合されます。このシナリオでは、SonicWave はクライアントに EAP 認証を提供し、認証システムと認証サーバの両方として同時に機能します。再接続時の動作を高速化するために、LDAP キャッシュと TLS キャッシュがサポートされています。

この機能を設定するために必要なこと:

- WLAN ゾーンにインターフェースがあって、そこでサブネットに 1 つ以上のローカル RADIUS サーバを設定すること。これらは SonicWave ローカル RADIUS サーバです。
- WLAN ゾーンの設定に関連して「**RADIUS サーバ**」画面の「**ローカル RADIUS サーバを有効にする**」オプションを選択すること。このオプションは、この機能を有効にするかどうかを制御します。
- SonicWave プロファイルに関連して「**無線の基本**」画面で以下を設定すること:
    - いずれかの **WPA2 - EAP** を「**認証種別**」で選択

      「**RADIUS サーバの設定**」セクションと「**設定**」ボタンが表示され、ローカル RADIUS サーバの設定を行うことができます。詳細については、「RADIUS サーバの設定」を参照してください。

- いずれかの**ローカル RADIUS サーバ** オプションを「**認証バランス方式**」で選択



ローカル RADIUS サーバ優先 - このオプションを選択すると、クライアントが認証を試みたとき、最初にローカル RADIUS サーバが使用されます。認証に失敗すると、認証要求はリモート RADIUS サーバに送信されます。

リモート RADIUS サーバのみ - リモート RADIUS サーバのみを認証に使用します。

ローカル RADIUS サーバのみ - ローカル RADIUS サーバのみを認証に使用します。

フェイルオーバー 方式としてローカル RADIUS サーバ - リモート RADIUS サーバがダウンしたとき、ローカル RADIUS サーバが自動的に使用されます。

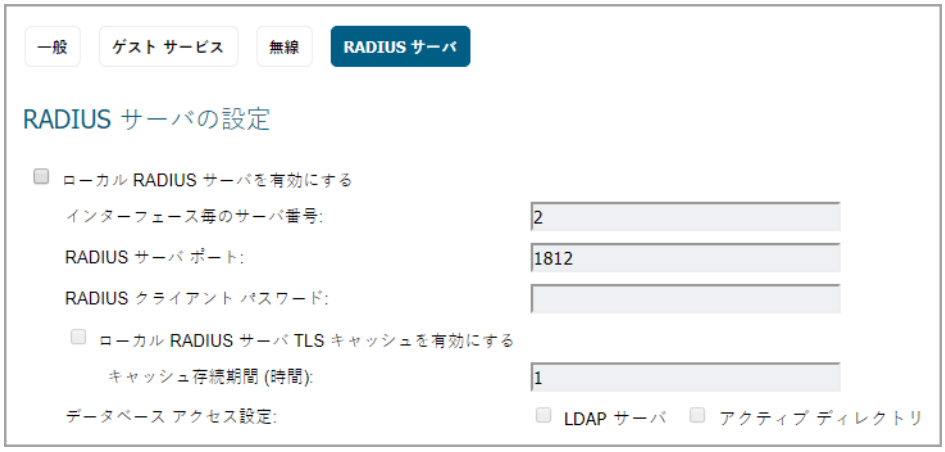
- NAT ポリシー、アクセス ルール、アドレス グループ、RADIUS プール - 自動的に設定される

SonicWave でローカル RADIUS サーバを有効にすると、NAT ポリシーとアクセス ルールが自動的に作成されます。SonicOS NAT モジュールにはフェイルオーバーと負荷分散の機能があるため、RADIUS サーバ プールがサポートされています。ローカル RADIUS サーバが設定された追加的な SonicWave をこのプールに追加できます。複数のローカル RADIUS サーバによって、フェイルオーバー メカニズムが提供され、ネットワーク パフォーマンスが最適化されます。

「**ローカル RADIUS サーバを有効にする**」オプションその他の項目の設定は、「**管理 | システム セットアップ | ネットワーク > ゾーン**」ページから ***WLAN ゾーン***を設定するときに使用可能となる「**RADIUS サーバ**」画面で行われます。この画面には、インターフェースあたりの RADIUS サーバ数、サーバ ポート、クライアント パスワード、TLS キャッシュ、および LDAP または Active Directory アクセス設定を設定するためのオプションがあります。SonicWave でローカル RADIUS サーバを有効にすると、設定されている RADIUS サーバ ポートとクライアント パスワードがその SonicWave で使用されます。

メモ：SonicWave DNS サーバは、LDAP サーバまたは Active Directory サーバ ドメインの名前を解決できる必要があります。

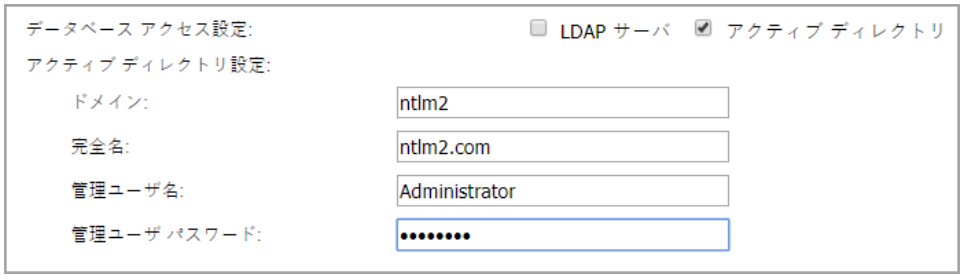
「**インターフェースあたりのサーバ数**」オプションは、このゾーンの特定インターフェースの配下にあるローカル RADIUS サーバ数を制御します。この値を増やすと、RADIUS プールに追加できる SonicWave が増えます。最小値は 1 で、最大値は WLAN ゾーンのインターフェースあたりの SonicWave の最大数と等しくなります。このオプションで設定する値は、接続されている SonicWave 数よりも小さいので、ローカル RADIUS サーバとして設定した特定の SonicWave は固定されません。



「**ローカル RADIUS サーバ TLS キャッシュを有効にする**」オプションが有効になっている場合、クライアントとサーバは TLS セッションの鍵をキャッシュし、これを使用してクライアントのる認証要求と RADIUS サーバの応答の間の時間的な遅延を減らすことができます。クライアントは高速再接続も実行できます。有効にすると、「**キャッシュ持続期間 (時間)**」オプションでキャッシュ項目の保存時間数を設定できます。キャッシュの持続時間は、1 時間から 24 時間の範囲で指定できます。

LDAP **データベース アクセス設定**の例を以下に示します。

Active Directory **データベース アクセス設定**の例を以下に示します。



セキュリティ装置の起動時に、「**ローカル RADIUS サーバを有効にする**」が WLAN ゾーンで有効になっていると、アドレス オブジェクト、RADIUS プール、NAT ポリシー、およびアクセス ルールが作成されるはずです。RADIUS プールの名前は、インターフェース名と「Radius Pool」の組み合わせです。例えば、`X2 Radius Pool` のようになります。RADIUSサーバとして動作する SonicWave の新しいアドレス オブジェクトが自動的に作成されます。これは、SonicWave のインターフェース名と MAC アドレスに基づいて名前が付けられます。例えば、`X2 18:b1:69:7b:75:2e` のようになります。利用可能なシートがあれば、このアドレス オブジェクトは RADIUS プールに追加されます。

「**ローカル RADIUS サーバを有効にする**」が無効になっている場合、SonicWave アドレス オブジェクト、RADIUS プール、NAT ポリシー、およびアクセス ルールは削除されます。また、restApi による DELETE コマンドが RADIUS プール内の SonicWave に送信され、ローカル RADIUS サーバは停止します。

WLAN ゾーンが編集されると、NAT ポリシーとアクセス ルールは削除され、再作成されます。「**ローカル RADIUS サーバを有効にする**」が無効になっていない限り、RADIUS プールは常に存在します。

インターフェースが変更された場合、インターフェースがまだ WLAN ゾーンにバインドされていると、NAT ポリシー、アクセス ルール、および RADIUS プールは削除され、再度作成されます。

RADIUS サーバの設定

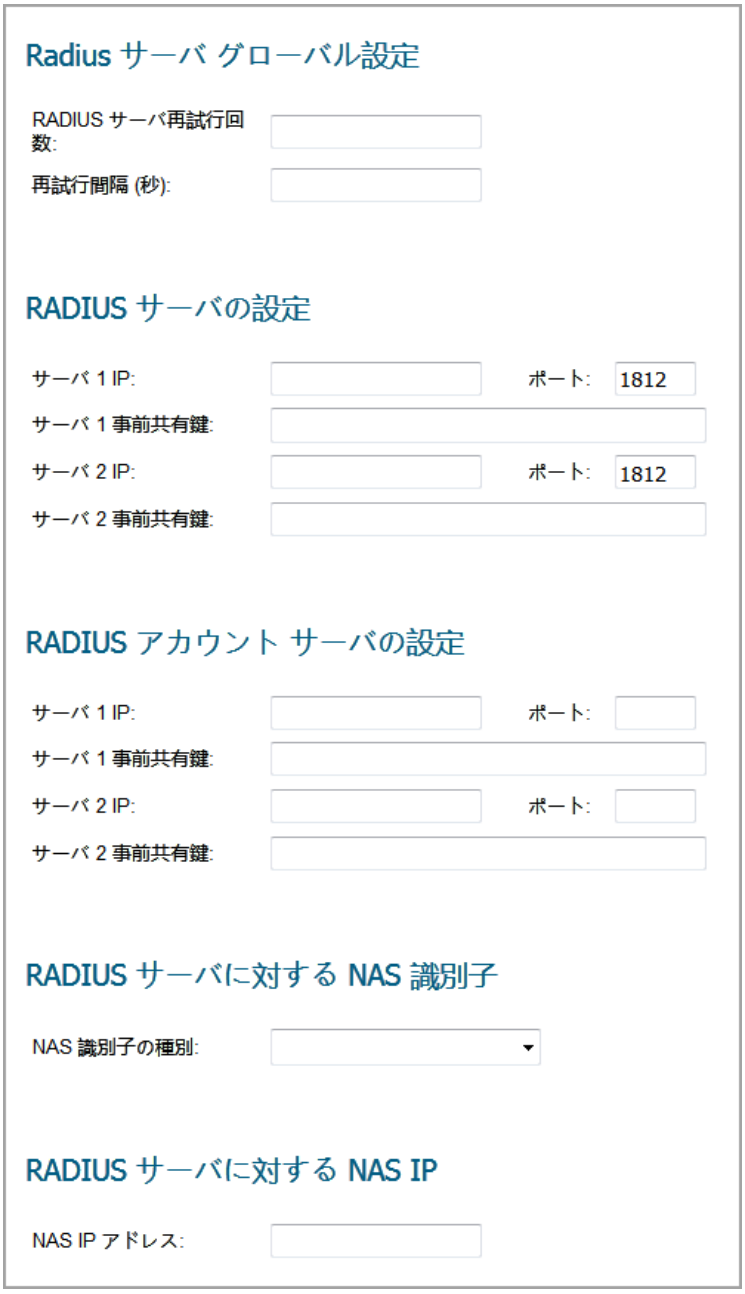
「**WPA2 - EAP**」または「**WPA2 - 自動 - EAP**」を「**無線セキュリティ**」セクションで選択した場合、「**RADIUS サーバの設定**」セクションが表示され、RADIUS サーバによる認証鍵の生成に関する設定を行うことができます。サーバはこのために、また、SonicWall 装置と通信できるよう設定されていなくてはなりません。

RADIUS サーバ設定を行うには、以下の手順に従います。

1 「**設定**」ボタンを選択します。「**RADIUS サーバの設定**」ダイアログが表示されます。このダイアログ上のオプションは、SonicPoint/SonicWave の種別

SonicPointNDR または SonicPoint N

SonicPointACe/ACi/N2 - SonicWave



2 「**RADIUS サーバ再試行回数**」フィールドに、他の RADIUS サーバにフェイルオーバーする前に、ファイアウォールが接続を試行する回数を 1 ～ 10 の数値で入力します。

3 「**再試行間隔 (秒)**」フィールドに、次の再試行まで待つ時間を 0 ～ 60 秒で入力します。既定値は **0** で、間隔を置かずに再試行することを意味します。

4 以下のテーブルの説明に従って、**RADIUS サーバの設定** を定義します。

RADIUS 認証サーバの設定

オプション	説明
サーバ 1 IP	RADIUS 認証サーバの名前/場所
サーバ 1 パスコード	RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポート。既定のポートは **1812** です。
サーバ 1 事前共有鍵	RADIUS サーバ用のシークレット パスコード
サーバ 2	バックアップ RADIUS 認証サーバの名前/場所
サーバ 2 パスコード	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポート。既定のポートは **1812** です。
サーバ 2 事前共有鍵	バックアップ RADIUS 認証サーバ用のシークレット パスコード

5 RADIUS サーバを課金のために使用量を追跡するために利用するのであれば、RADIUS アカウント サーバをセットアップしてください。

RADIUS アカウント サーバの設定

オプション	説明
サーバ 1 IP	RADIUS 認証サーバの名前/場所
サーバ 1 パスコード	RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポート。
サーバ 1 事前共有鍵	RADIUS サーバ用のシークレット パスコード
サーバ 2	バックアップ RADIUS 認証サーバの名前/場所
サーバ 2 パスコード	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポート。
サーバ 2 事前共有鍵	バックアップ RADIUS 認証サーバ用のシークレット パスコード

6 NAS 識別子を RADIUS サーバに送信するには、「**NAS 識別子の種別**」ドロップダウン メニューから種別を選択します。

- **含まない** (既定)
- **SonicPoint の名前**
- **SonicPoint の MAC アドレス**
- **SSID** - SSID オプションが選択されている場合、RADIUS 認証メッセージと RADIUS アカウント メッセージの両方がアクセス ポイントまたは SSID を伝送します。

7 NAS の IP アドレスを RADIUS サーバに送信するには、「**NAS IP アドレス**」フィールドにアドレスを入力します。

8 「**OK**」を選択します。

ACL 強制

各 アクセス ポイント は、個別のアクセス制御リスト (ACL) をサポートして、より効率的な認証制御を提供できます。この ACL 機能は、現在 SonicOS で利用可能な無線 MAC フィルタ リストと同時に動作します。この ACL 強制機能を使って、ユーザは MAC フィルタ リストを有効/無効にする、許可リストを設定する、そして拒否リストを設定することが可能です。

MAC フィルタ リストの強制化を有効にする

1 「**MAC フィルタ リストを有効にする**」チェックボックスをオンにします。MAC フィルタ リストが有効な場合、他の設定項目も設定できるように表示されます。

2 「**許可リスト**」で、ドロップダウン リストからオプションを選択します。どの MAC アドレスにアクセスを許可するかを指定します。

アクセスさせたい MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。これを行うための情報については、「*SonicOS 6.5 ポリシー*」を参照してください。

3 「**拒否リスト**」で、ドロップダウン リストからオプションを選択します。どの MAC アドレスからのアクセスを拒否するかを指定します。

アクセスさせたくない MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。これを行うための情報については、「*SonicOS 6.5 ポリシー*」を参照してください。

4 **MIC 失敗 ACL ブラックリストを有効にする** 場合、チェックボックスをオンにします。

5 **MIC 失敗頻度のしきい値** を、1 分間の回数に基づいて設定します。既定値は **3** です。

リモート MAC アドレス アクセス制御の設定

このオプションでは、RADIUS サーバによる、MAC ベースの認証ポリシーに基づく無線アクセス制御を強制することができます。

無線アクセス制御を許可するには、以下の手順に従います。

1 **リモート MAC アクセス制御** を有効にするチェックボックスをオンにします。

2 「**設定**」を選択します。

3 設定済でなければ、RADIUS サーバを「RADIUS サーバの設定」の説明に従ってセットアップします。

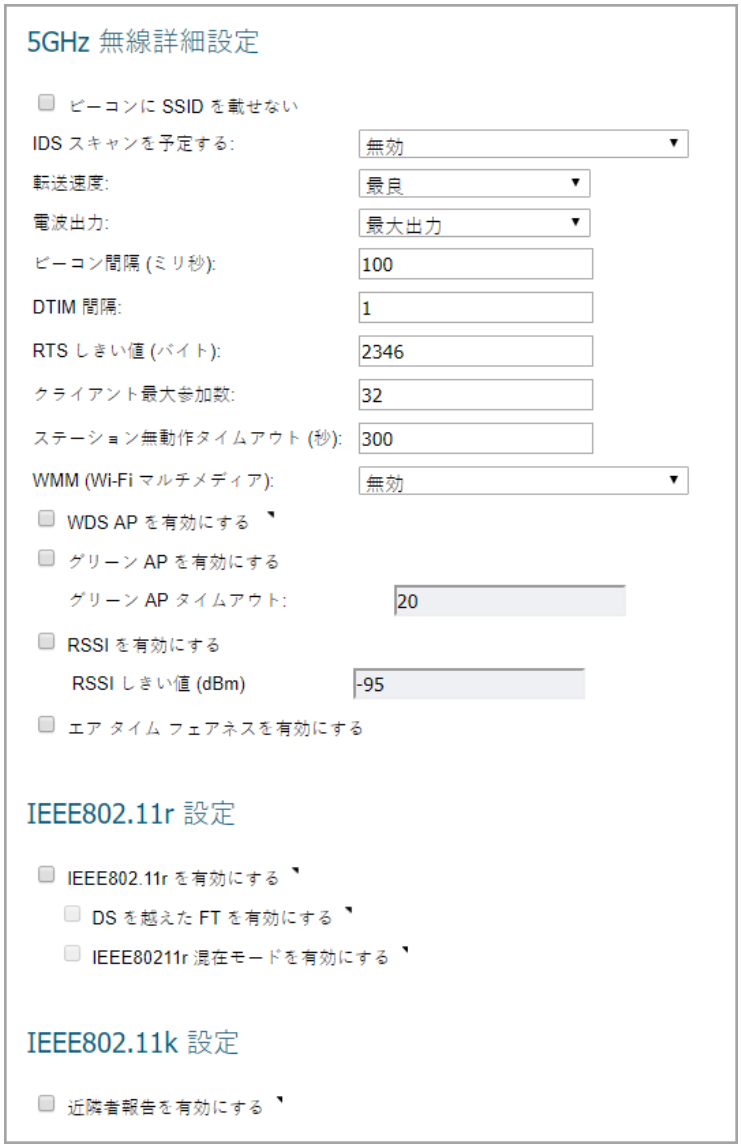
4 「**OK**」を選択します。

プロビジョニング プロファイルの 5GHz/2.4GHz 無線の詳細設定

これらの設定は、無線帯域の動作に影響します。SonicPoint/SonicWave は 2 種類の内蔵無線を搭載しているため、両方の帯域での送受信を同時に行うことができます。

「**5GHz 無線の詳細**」画面には、「**2.4GHz 無線の詳細**」画面と同じオプションに加えて、その他のオプションがあります。これらの画面は、さまざまなアクセス ポイント モデルで類似しています。相違点については、必要があれば手順の中で示します。

無線詳細設定



5GHz 無線/2.4GHz 無線の詳細設定を行うには:

1 必要に応じて、「**5GHz 無線の詳細**」または「**2.4GHz 無線の詳細**」を選択します。

2 **ビーコンに SSID を載せない** 場合にはチェックボックスをオンにします。こうすると、SSID が無線 SSID 名の通知の代わりにヌル SSID ビーコンを送信するようにします。ヌル SSID ビーコンを送信すると、接続する SSID を無線クライアントに強制的に知らせることができます。このオプションは既定でオフになっています。

3 「**IDS スキャンを予定する**」ドロップダウン メニューから、IDS (侵入検知サービス) スキャンのスケジュールを選択します。

無線接続が破棄されるという不都合を最小限に抑えるために、無線ネットワークの需要が比較的少ない時間を選択します。「**スケジュールの作成**」を選択して独自のスケジュールを作成したり、既定の設定である「**無効**」を選択してこの機能を無効にしたりすることができます。

メモ：IDS は、無線の脅威からネットワークを保護するためのさまざまな侵入検知機能を備えます。この機能によって、許可されたアクセス ポイント、RF 媒体、有線ネットワークで構成される WLAN インフラに対する攻撃が検知されます。許可されている有効な AP は、WLAN インフラに属するアクセス ポイントとして定義されます。アクセス ポイントは、SonicPoint、SonicWave、またはサードパーティのアクセス ポイントです。

4 「**転送速度**」ドロップダウン メニューから、データが送受信される速度を選択します。「**最良**」(既定) では、電磁波妨害やその他の要因を考慮したうえで、その地域で利用できる最適な速度が自動的に選択されます。

5 「**電波出力**」ドロップダウン メニューから、電波出力を選択します。電波出力は SonicPoint の範囲に影響します。

- **最大出力** (既定)
- **1/2 出力 (-3 dB)**
- **1/4 出力 (-6 dB)**
- **1/8 出力 (-9 dB)**
- **最低出力**

6 SonicPoint NDR を設定する場合は、「**使用するアンテナ**」ドロップダウン メニューから、「**最良**」(既定値) を選択します。

使用するアンテナ 設定は、アクセス ポイント がデータの送受信に使用するアンテナを決定します。「**最良**」を選択すると、強度が最も高く、劣化していない信号を受信したアンテナが アクセス ポイント によって自動的に選択されます。

7 「**ビーコン間隔 (ミリ秒)**」フィールドに、無線 SSID ビーコンを送出する間隔をミリ秒単位で入力します。最小間隔は 100 ミリ秒 (既定値)、最大間隔は 1000 ミリ秒です。

8 「**DTIM 間隔**」フィールドに、DTIM 間隔をミリ秒で入力します。フレーム数の最小値は 1 (既定値)、最大値は 255 です。

マルチキャスト パケットを受信する 802.11 省電力モードのクライアントに対し、「**DTIM 間隔**」は、DTIM (Delivery Traffic Indication Message) を送信する前に待つビーコン フレーム数を指定します。

9 SonicPointNDR を設定する場合、「**断片化のしきい値 (バイト)**」フィールドに、ネットワークで許容する断片化データのバイト数を入力します。

断片化のしきい値は、最大フレーム サイズを制限します。フレーム サイズを制限すると、フレーム送信に要する時間が短くなるため、フレームが破損する確率が低下します (その代わりに、データ オーバーヘッドは高くなります)。無線フレームの断片化は、RF 干渉が存在する場所や、無線通信範囲の電波が弱い場所において、信頼性とスループットを向上させます。しきい値が低いほど、より細かく断片化されます。最小値は 256 バイト、最大値は 2346 バイト (既定値) です。

10 「**RTS しきい値 (バイト)**」フィールドに、パケット送信の前に送信する RTS (Request to Send: 送信要求) のパケット サイズのしきい値をバイト単位で入力します。

RTS を送信すると、クライアントが同じアクセス ポイントの範囲内にあるが互いの範囲内にあるとは限らないという状況で、無線の衝突が生じないようにすることができます。しきい値の最小値は 256 バイト、最大値は 2346 バイト (既定値) です。

11 「**クライアント最大参加数**」フィールドに、このプロファイルを使用する各 アクセス ポイントに、この無線で同時にサポート させたいクライアントの最大数を入力します。クライアント数の最小値は 1、最大値は 128、既定値は **32** です。

12 「**ステーション無動作タイムアウト (秒)**」フィールドに、無線クライアントの無動作の最大時間を秒単位で入力します。この時間が経過すると、アクセス ポイント はその無線クライアントを期限切れにします。最小値は 60 秒、最大値は 36000 秒、既定値は **300** 秒です。

13 「**2.4GHz 無線の詳細**」画面の設定を行う場合は、そのウィンドウに固有の以下の設定を定義してください。そうでなければ次のステップに進んでください。

オプション	設定
プリアンブル長	ドロップダウン メニューから次のいずれかを選択します。 • **長い** (既定) • **短い**
「保護モード」	ドロップダウン メニューから次のいずれかを選択します。 • **なし** • **常に** • **自動**
「保護速度」	ドロップダウン メニューから次のいずれかを選択します。 • **1 Mbps** (既定) • **2 Mbps** • **5 Mbps** • **11 Mbps**
「保護種別」	ドロップダウン メニューから次のいずれかを選択します。 • **CTS のみ** (既定) • **RTS と CTS**
Short Slot Time を有効にする	クライアントによる不参加と再参加を迅速に行えるようにします。このオプションを指定すると、アクセス ポイントがパケットを LAN にリレーする前に待機する時間を短くすることによって、802.11n/g 無線帯域上のスループットを上げることができます。
802.11b クライアントの接続を許可しない	ターボ G モードを使用する (したがって 802.11b クライアントの接続を許可しない) 場合に、これを使用します。このオプションを指定すると、無線接続が 802.11g と 802.11n のクライアントのみに制限されます。

14 「**WMM (Wi-Fi マルチメディア)**」ドロップダウン メニューで、WMM プロファイルをこのプロファイルに関連付けるかどうかを選択します。

- **無効** (既定)
- **WMM プロファイルの作成**詳細については、「Wi-Fi マルチメディアの設定」を参照してください。
- 設定済みの WMM プロファイル

15 「**WDS AP を有効にする**」チェックボックスをオンにします。これを利用すると、複数のアクセス ポイントを使用して、以前のような各アクセス ポイントを接続する有線バックボーンを必要とせずに、無線ネットワークを拡大できるようになります。

16 必要に応じて、「**グリーン AP を有効にする**」を選択して、アクセス ポイント 無線がスリープモードに入ることを許可します。これによって、アクティブに接続するクライアントが存在しない場合の電力が抑えられます。いずれかのクライアントが接続を試みると、アクセス ポイント は直ちに最大出力モードに入ります。緑の AP は、5GHz 無線と 2.4GHz 無線の各無線に対してそれぞれ個別に設定できます。

17 「**グリーン AP タイムアウト**」フィールドに、アクティブな接続が存在しない場合にスリープ モードに入るまでにアクセス ポイントが待機する時間を入力します。この遷移時間の範囲は 20 ～ 65535 秒で、既定値は **20** 秒です。

18 SonicWave またはSonicPoint ACe/ACi/N2 プロファイルを設定する場合は、「**RSSI を有効にする**」チェックボックスをオンにして RSSI しきい値を有効にします。信号強度がしきい値を下回るクライアントは、アクセス ポイントによって関連付けが解除されるため、より近いアクセス ポイントに関連付けられます。 このオプションは、既定では選択されていません。

19 「**RSSI を有効にする**」が選択されている場合は、しきい値を負の値として「**RSSI しきい値 (dBm)**」フィールドに入力します。既定値は -95 dBm です。RSSI しきい値の詳細については、「RSSI しきい値の設定 (204 ページ)」を参照してください。

20 SonicWave 機器を設定する場合、「**エア タイム フェアネスを有効にする**」チェックボックスをオンにしてください。

この機能は、既定では無効になっています。有効にすると、5GHz 帯を使用できる機器に対して 5GHz 帯を使用させます。通常、5GHz 帯の方がトラフィックが少なく、干渉も少ないためです。信号強度または信号品質が 2.4GHz 帯の方が良好である場合、トラフィックはそちらの帯域を使用させます。目的は、両方の帯域を最も有効な方法で使用することです。

21 「**IEEE802.11r 設定**」で、「**IEEE802.11r を有効にする**」チェックボックスをオンにして、安全で高速なローミングを有効にします。「**IEEE802.11r を有効にする**」が選択されている場合は、その他のオプションを選択できます。

- **DS を介した FT の有効化** - DS を介した高速移行を有効にします。
- **IEEE802.11r 混合モードを有効にする** - 混合モードでの高速移行を有効にします。

これらのオプションの詳細については、「安全で高速なローミングのための IEEE802.11r 設定 (205 ページ)」を参照してください。

22 「**IEEE802.11k 設定**」で、「**近隣者報告を有効にする**」チェックボックスをオンにして、近隣アクセス ポイントについての情報の収集を有効にします。このオプションは、既定では選択されていません。詳細については、「動的無線管理のための IEEE802.11k 設定 (205 ページ)」を参照してください。

23 「**IEEE802.11v 設定**」で、「**BSS 移行管理を有効にする**」チェックボックスをオンにして、クライアントがアクセス ポイントにクエリを送信した場合にアクセス ポイントが音声クライアントに特定のアクセス ポイントへの移行を要求できるようにします。このオプションは、既定では選択されていません。詳細については、「動的環境管理のための IEEE802.11v 設定 (206 ページ)」を参照してください。

24 「**IEEE802.11v 設定**」で、「**WNM スリープ モードを有効にする**」チェックボックスをオンにして、非アクセス ポイント ステーションが指定の時間だけスリープすることをアクセス ポイントに通知できるようにします。このオプションは、既定では選択されていません。詳細については、「動的環境管理のための IEEE802.11v 設定 (206 ページ)」を参照してください。

RSSI しきい値の設定

エリア全体に適切な WiFi カバレッジを提供するために複数のアクセス ポイントを必要とするほど大きいエリアでは、WiFi クライアン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が期待されます。残念ながら、多くの WiFi クライアントは、通常はより良い選択である近くのアクセス ポイントに移動するのではなく、関連付けられた元のアクセス ポイントに固執する傾向があります。これはスティッキ動作と呼ばれ、低い RSSI (受信信号強度インジケータ) と高い SNR (信号対雑音比) をもたらします。クライアントが移動する元のアクセス ポイントから離れるほど、その RSSI は弱くな

り、SNR は悪くなります。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します。データレートが低いと、同じ情報を転送するための通信時間が長くなり、チャンネル使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、結果として生じる RF スペースは誰にとってもより良いものになります。

SonicOS 6.5.2 以降では、RSSI しきい値がサポートされています。クライアントがアクセス ポイントから見て一定の RSSI レベルに達すると、アクセス ポイントはクライアントから切り離され、クライアントはより近いアクセス ポイントに関連付けられます。RSSI しきい値は設定可能です。

RSSI 測定値は、アンテナおよびケーブル レベルで損失が発生した後のデバイスで受信した信号の相対的な品質を表します。RSSI 値が高いほど、信号は強くなります。負の値で測定した場合、ゼロに近い値は通常、より良い信号を意味します。例として、-50 dBm は非常に良好な信号であり、-75 dBm はかなり妥当であり、-100 dBm はまったく信号がありません。

安全で高速なローミングのための IEEE802.11r 設定

IEEE 802.11 WiFi の多くの実装の有効範囲はわずか数百メートルであるため、通信を維持するには、移動中のデバイスをあるアクセス 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。自動車環境では、5-10 秒ごとにハンドオフが起こる可能性があります。

ハンドオフは現在の標準で既にサポートされています。802.11 でのハンドオフの基本アーキテクチャは、802.11r を使用しても使用しなくても変わりません。モバイル デバイスは、ハンドオフするタイミングとハンドオフするアクセス ポイントの決定を完全に任されます。802.11 の初期の頃、ハンドオフはモバイル デバイスにとってはるかに簡単なタスクでした。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必要なメッセージは 4 つだけです (クライアントから以前のアクセス ポイントに送信される可能性のあるオプションの「I'm leaving」メッセージ [認証解除および不参加パケット] もカウントする場合は 5)。しかし、802.1X 認証を備えた 802.11i や、アドミッション コントロール リクエストを備えた 802.11e または WMM などの追加機能が標準に追加されたため、必要なメッセージの数は劇的に増加しました。これらの追加メッセージが交換されている間、音声通話からのトラフィックを含むモバイル デバイスのトラフィックは処理できず、ユーザが経験する損失は数秒に及ぶ可能性があります。一般的に、エッジ ネットワークが音声コールに導入す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のためにハンドオフ プロセスに追加された追加の負荷を取り除いて、元の 4 メッセージ交換の状態に戻します。この方法では、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ります。

802.11r 標準で現在想定されている主なアプリケーションは、標準のセルラー ネットワークの代わりに（またはそれに加えて）ワイヤレス 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 Voice over IP (VOIP) です。

動的無線管理のための IEEE802.11k 設定

「5GHz または 2.4GHz 無線の詳細」画面の「**IEEE802.11k 設定**」セクションには、「**近隣レポートを有効にする**」オプションがあります。このオプションを有効にすると、802.11 標準の IEEE802.11k 改正で定義されているように、アクセス ポイントが無線測定値を収集します。

近隣レポート要求は、クライアントからアクセス ポイントに送信されます。アクセス ポイントは、クライアントが再参加する既知の候補である隣接アクセス ポイントに関する情報を含む近隣レポートを返します (クライアントがそうすることを選択した場合)。したがって、近隣レポート要求/レポート ペアにより、クライアントは、現在関連付けられているアクセス ポイントの近隣アクセス ポイント に関する情報を収集できます。この情報は、ローミング中に新しい接続点の潜在的な候補の識別として使用できます。

近隣レポート要求/レポートの利点は次のとおりです。

- **スキャンの高速化** - クライアントが時間のかかるスキャンア クティビティ (アクセス ポイント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) に関与する代わりに、クライアントはそのリストを既知の利用可能な近隣に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。
- **クライアントの電力消費を削減** - 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は消費されます。近隣レポートはローミング前に情報を提供するため、消費される電力が少なくなる可能性があります。
- **WLAN エアタイムのより効率的な使用** - アクティブ スキャンは、クライアント リソース (CPU、メモリ、無線など) の観点から時間がかかるだけでなく、エアタイムも消費します。例えば、近隣対応でないクライアントは、いわゆるワイルドカード プローブ要求に関与する可能性があります (一部のクライアントはこれらをバーストします)。このシナリオでは、通常、プローブ要求をリッスンするすべてのアクセス ポイントがプローブ応答を生成します。つまり、単一のクライアントの場合、N 個のアクセス ポイントが 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 プローブを行う場合、クライアントが近隣要求を使用していないという理由だけで、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 全体に悪影響を及ぼします。

動的環境管理のための IEEE802.11v 設定

802.11v は、IEEE802.11 ワイヤレス ネットワーク管理 (改正 8) を指します。これは、ワイヤレス ネットワークに接続しているときにクライアント デバイスを構成できるようにするための IEEE 802.11 標準の修正です。WNM（ワイヤレス ネットワーク管理）をサポートするステーションは、相互 (アクセス ポイントとワイヤレス クライアント) に情報を交換してワイヤレス ネットワークのパフォーマンスを向上させることができます。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 ネットワークを認識させて、ワイヤレス ネットワークの全体的な改善を促進できます。

ステーションは WNM プロトコルを使用して操作データを交換し、各ステーションがネットワークの状態を認識できるようにして、ステーションがネットワークのトポロジと状態をより認識できるようにします。WNM プロトコルは、ステーションが共存干渉の存在を認識し、ステーションがネットワーク条件に基づいて 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。

ネットワーク状態に関する情報の提供に加えて、WNM は位置情報の交換、同じワイヤレス インフラストラクチャでの複数の BSSID 機能のサポート、グループ アドレス指定フレームの効率的な配信のサポート、WNM スリープ モード (STA が AP からフレームを受信せずに長時間スリープできる) の有効化の手段も提供します。

BSS 最大アイドル期間管理は、SonicWall SonicPoint によってサポートされています。SonicWave は、ワイヤレス 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 移行管理を有効にする** - 特定のアクセス ポイントへの移行を音声クライアントに要求するアクセス ポイントを有効にするか、ネットワーク負荷分散または BSS 終了のために音声クライアントに一連の優先アクセス ポイントを提案します。これにより、音声クライアントは、そのクライアントがローミングするときに移行する必要がある最適なアクセス ポイントを識別できます。

  BSS 移行機能は、個々の音声トラフィックの負荷を ESS 内のより適切な関連付けポイントに（移行を介して）シフトすることにより、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 を改善できます。

  802.11v BSS 移行管理要求は、クライアントに提供される提案です。クライアントは、提案に従うかどうかを独自に決定できます。

BSS 移行管理は、次のフレーム種別を使用します。

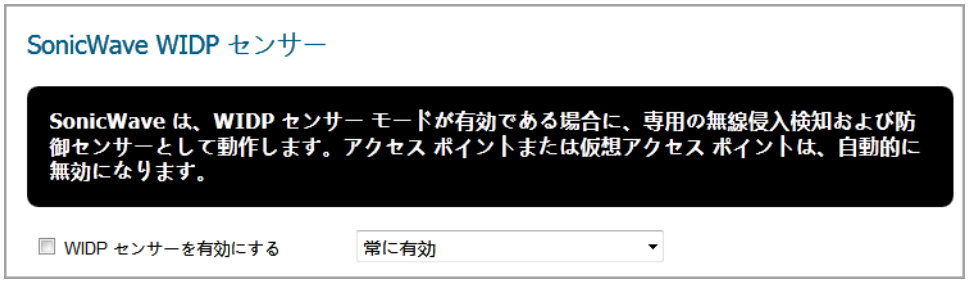
- **クエリ** - 関連アクセス ポイントが BSS 移行機能のサポートを示している場合、BSS 移行管理をサポートする音声クライアントが BSS 移行候補リストをその関連アクセス ポイントに要求するときクエリ フレームを送信します。
- **要求** - BSS 移行管理をサポートするアクセス ポイントは、BSS 移行管理クエリ フレームに BSS 移行管理要求フレームで応答します。
- **応答** - 応答フレームが音声クライアントによってアクセス ポイントに返され、遷移を受け入れるか拒否するかが通知されます。

- **WNM スリープ モード** - 非アクセス ポイント ステーションがすべての配信 DTIM (Delivery Traffic Indication Message) ビーコン フレームをリッスンする必要がなく、GTK/IGTK (Group Temporal Key/Integrity Group Temporal Key) の更新を実行しない非アクセス ポイント ステーション用の拡張省電力モード。

  WNM-Sleep モードは、非アクセス ポイント ステーションがアクセス ポイントに指定の時間だけスリープすることを通知できるようにします。これにより、非アクセス ポイント ステーションは電力消費を削減し、ステーションにアクセス ポイントとの間で送受信するトラフィックがない間、関連付けられたままになります。

重要：WNM-Sleep モードが有効で、ステーションが WNM-Sleep 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 (Key Reinstallation Attack) を回避するためにステーションを更新します。

プロビジョニング プロファイルの WIDP のセンサー設定



「**センサー**」画面では、「無線侵入検知と防御 (WIDP)」モードを有効または無効にできます。SonicOS 6.5.3 以降では、SonicWave 装置はアクセス ポイントとしても、SonicWall ネットワークに接続された不正アクセス ポイントを検知するセンサーとしても機能します。

以前のリリースでは、このオプションが選択されると、アクセス ポイント または仮想アクセス ポイントの機能は自動的に無効になります。

センサー画面オプションを設定するには:

1 「**WIDP センサーを有効にする**」を選択すると、アクセス ポイント は WIDP センサーとして動作します。このオプションは、既定では選択されていません。

2 アクセス ポイント が WIDP センサーとして動作する時間のスケジュールをドロップダウン メニューから選択するか、「**新しいスケジュールの作成...**」を選択して別の時間を指定します。既定は「**常に有効**」です。

プロビジョニング プロファイルのメッシュ ネットワーク設定

この機能は、大規模なカバレッジ エリア全体にスケーラブルで安全なワイヤレス ネットワーク インフラストラクチャを提供します。この機能を利用して、SonicWave アクセス ポイントを配備および管理できます。

トピック:

メッシュ ネットワークのセットアップ

メッシュ ネットワークをセットアップするには、以下の手順に従います。

1 「マルチホップ メッシュ ネットワークの有効化」の説明に従って、ファイアウォールの SonicWave プロファイルでメッシュを有効にします。

2 各 SonicWave を、イーサネット ケーブルによってこのファイアウォールに接続します。

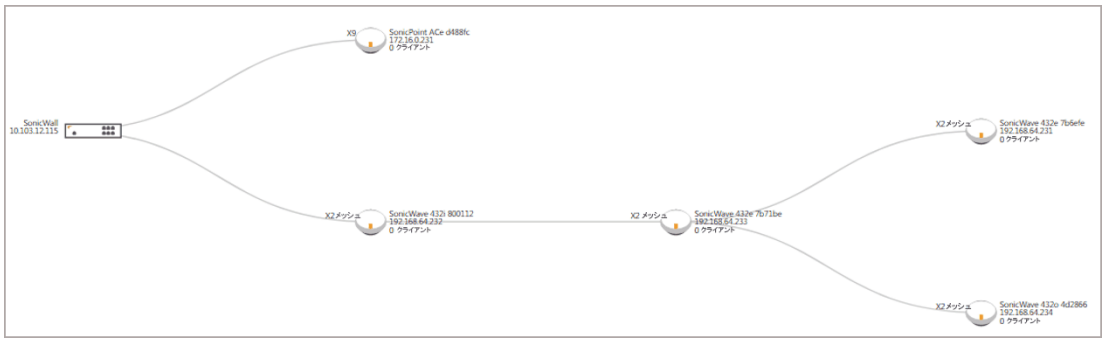
3 SonicWave の状態が「利用可能」になったら、その装置からケーブルを外します。

4 1 つの SonicWave をファイアウォールに接続したままにします。

5 切断した SonicWave を、所定の場所に移動します。

6 すべての SonicWave の電源を入れます。

7 ネットワークを表示するには、「**管理 | 接続性 > アクセス ポイント > トポロジ表示**」に移動します。



マルチホップ メッシュ ネットワークの有効化

マルチホップ メッシュ ネットワークを有効にするには、以下の手順に従います。

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

2 「**SonicWave プロビジョニング プロファイル**」ボタンを選択します。

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

4 「**メッシュ ネットワーク**」を選択します。

5 「**メッシュ無線**」から、メッシュ ネットワークに使用する無線を選択します。

- **5GHZ 無線**
- **2.4GHZ 無線**

6 SonicPointAC の無線帯域メッシュを有効にするには、「**メッシュを有効にする**」を選択します。

7 「**メッシュ SSID**」に、WLAN ネットワークの SSID を入力します。

8 「**メッシュ PSK**」に、事前共有鍵を入力します。

9 「**OK**」を選択します。

アクティブ/アクティブ クラスタリング フルメッシュ

アクティブ/アクティブ クラスタリングのフルメッシュ設定は、アクティブ/アクティブ クラスタリングの設定オプションを強化したもので、ネットワーク内のあらゆる単一障害点を回避します。ファイアウォールをはじめとするすべてのネットワーク機器は、完全な冗長化のために連携されます。フルメッシュでは、機器 (セキュリティ装置/スイッチ/ルータ) であれリンクであれ、一切の単一障害点が配備に存在しないことが保証されます。すべての機器は、接続先の機器に二重に配線されます。フルメッシュによるアクティブ/アクティブ クラスタリングは、実現可能な最高レベルの可用性と高いパフォーマンスを提供します。「アクティブ/アクティブ クラスタリング フル メッシュのメリット」を参照してください。

重要：セキュリティ装置のアップストリーム側ネットワーク内にあるルータは、Virtual Router Redundancy Protocol (VRRP) 向けにあらかじめ設定されている必要があります。

フル メッシュ配備では、ポート冗長化が有効かつ実現されている必要があります。

アクティブ/アクティブ クラスタリング フル メッシュのメリット

コア ネットワーク内に単一障害点が存在しない	アクティブ/アクティブ クラスタリング フルメッシュ配備では、セキュリティ装置だけでなく、コア ネットワーク全体にわたって単一障害点が存在しません。パス上のスイッチ、ルータ、セキュリティ装置に同時に障害が発生した場合でも、トラフィック フローの代替パスが必ず利用できるので、最高レベルの可用性を実現できます。
ポート冗長化	アクティブ/アクティブ クラスタリング フルメッシュでは、各クラスタ ノード内の HA 冗長化や、クラスタ内のノード レベルの冗長化に加え、冗長ポートも利用します。ポート冗長化では、プライマリ ポートに障害が発生した場合、バックアップ リンクがトランスペアレントな形で処理を引き継ぎます。この場合、機器レベルのフェイルオーバーは必要ありません。

プロビジョニング プロファイルの 3G/4G/LTE WWAN 設定

メモ：USB モデムを設定しない場合、このセクションはスキップできます。

この機能は、無線 アクセス ポイント を SonicWave 機器のように使用するファイアウォール装置に、追加の無線 WAN ソリューションを提供するものです。USB モデム機器を SonicWave に接続すると、ダイアルアップ動作を行ってインターネットに接続します。接続すると、SonicWave はファイアウォールの WWAN 装置として機能し、WAN アクセスを提供します。

モデムを最初に設定する場合、このオプションの自動発見機能を利用するために、ウィザードを使用することができます。

トピック:

- 3G/4G/LTE WWAN プロファイルの手動設定
- 3G/4G/LTE WWAN ウィザードの使用
- 複数の USB モデム間の負荷分散の設定

3G/4G/LTE WWAN プロファイルの手動設定

3G/4G/LTE WWAN プロファイルを手動で設定したり、手動で変更したりするには、以下の手順に従ってください。

モデムを WWAN として手動で設定するには、以下の手順に従ってください。

1 「**3G/4GWWAN**」をクリックします。

2 「**3G/4G/LTE モデムを有効にする**」チェック ボックスをオンにします。

3 **WAN VLAN インターフェースへの関連付け** ドロップダウン メニューから VLAN インターフェースを選択します。

ドロップダウン メニューにインターフェースが表示されない場合は、定義する必要があります。*SonicOS 6.5 システム設定* の ネットワーク > インターフェース を参照してください。

> **メモ**：VLAN インターフェースを構築する場合、ゾーンを WAN ゾーンにして、親インターフェースをアクセス ポイントが接続されている物理インターフェースにしてください。
>
> 3G USB モデムについては、**IP 割り当て**を**静的**に設定して、プライベート IP アドレスを割り当ててください。**ゲートウェイ**と **DNS サーバ** フィールドは空白のまま残します。
>
> 4G と QMI モデムについては、**IP 割り当て**を **DHCP** に設定します。

4 「**接続プロファイル**」セクションで、「**接続プロファイルを有効にする**」チェックボックスをオンにしてください。

> **メモ**：従来の 3G/4G モデムには、ダイアルアップ用の接続プロファイルを必要とするものがあります。

5 「**国**」フィールドには、アクセス ポイントが配備される国を選択してください。

6 ドロップダウン メニューから**サービス プロバイダ**を選択します。

7 ドロップダウン メニューから「**プラン種別**」を選択します。選択によって、他のフィールドが自動的に生成されます。

8 必要があれば**ユーザ名**と**パスワード**を適切なフィールドに入力します。

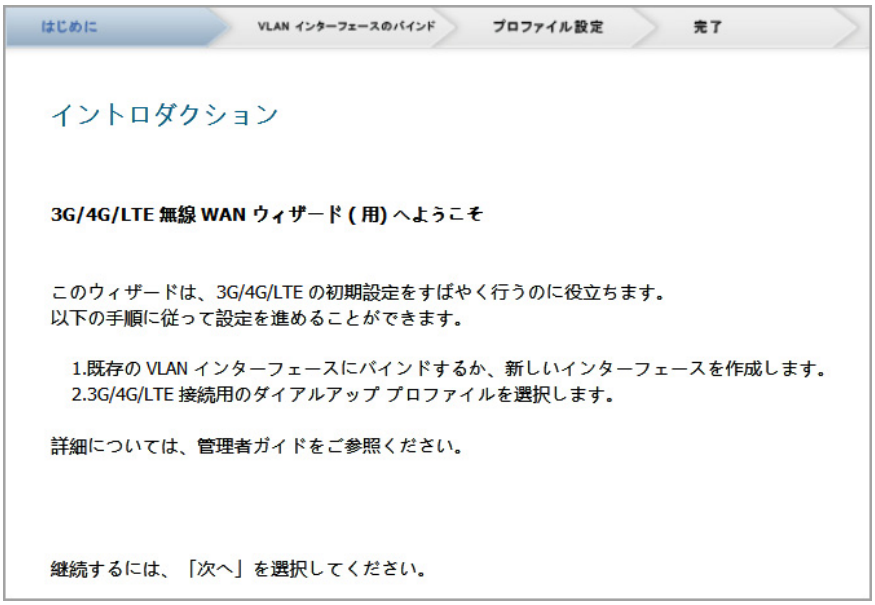
9 画面上のすべての設定が完了したら、「**OK**」を選択します。

3G/4G/LTE WWAN ウィザードの使用

ウィザードを使ってモデムを設定するには、以下の手順に従ってください。

1 「**3G/4GWWAN**」をクリックします。

2 一番下までスクロールし、「**3G/4G/LTE ウィザード**」を選択します。



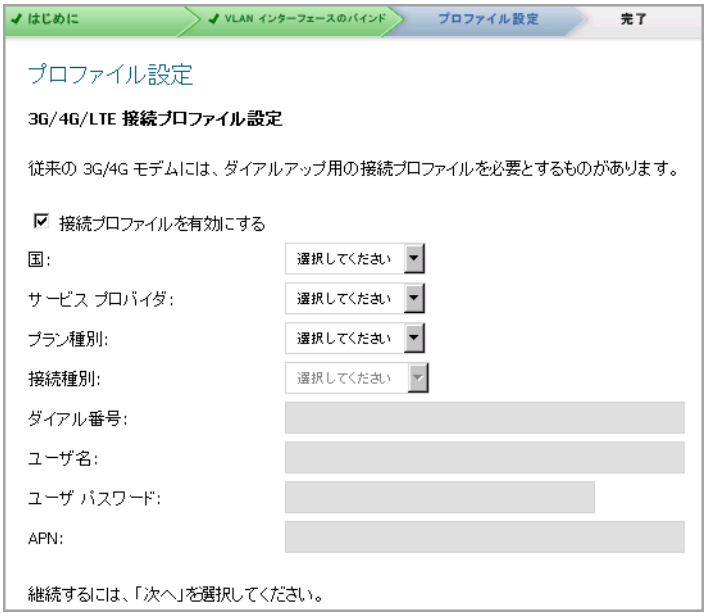
3 「**次へ**」ボタンを選択します。

4 「**VLAN インターフェース**」をドロップダウン メニューから選択するか、「**新しい VLAN インターフェースの作成**」のチェック ボックスをオンにします。

新しい VLAN インターフェースの作成を選択する場合は、残りのフィールドが有効化されます。要求されたデータを入力します。

メモ：「**IP 割り当て**」を「**DHCP**」に設定すると、IP アドレス、サブネット マスク、デフォルト ゲートウェイのフィールドは入力不可になります。

5 「**次へ**」ボタンを選択します。



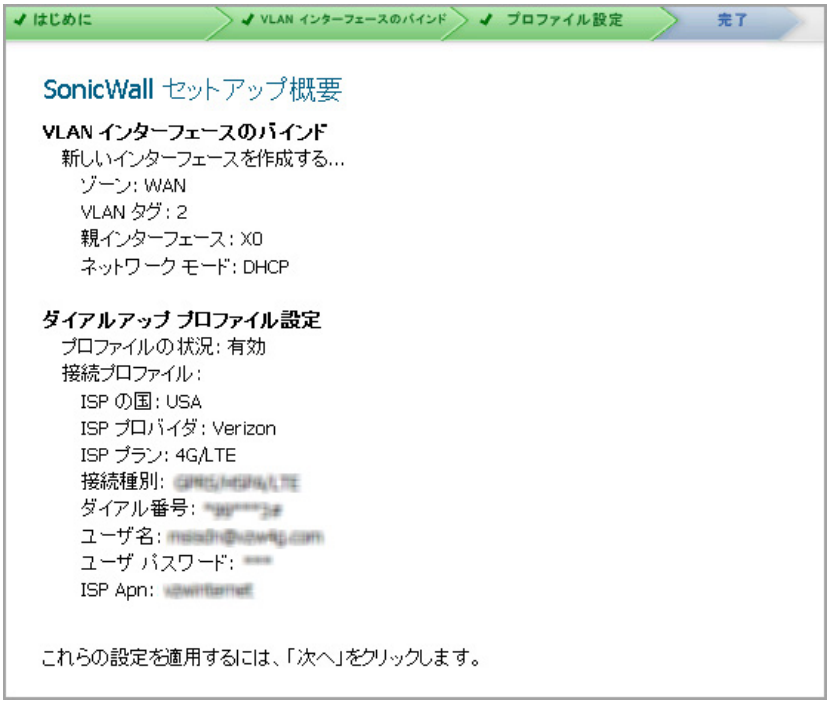
6 「**国**」フィールドには、アクセス ポイントが配備される国を選択してください。

7 ドロップダウン メニューから「**サービス プロバイダ**」を選択します。

8 ドロップダウン メニューから「**プラン種別**」を選択します。選択によって、他のフィールドが自動的に生成されます。

9 必要があれば**ユーザ名**と**パスワード**を適切なフィールドに入力します。

10 「**次へ**」ボタンを選択します。



11 再度「**次へ**」を選択して、設定を反映します。

複数の USB モデム間の負荷分散の設定

複数の SonicPoint/SonicWave および複数の 3G/4G モデム (それぞれ最低 2 台) が使用可能な場合、これらの SonicPoint/SonicWave およびモデムの複数のペア間で負荷分散を実行できます。

複数の 3G/4G モデムを使用して負荷分散を設定するには:

1 手動で、または 3G/4G/LTE ウィザードを使用して、SonicPoint/SonicWave と 3G/4G モデムの各ペアに一意の VLAN を割り当てます。

2 これらの VLAN インターフェースを「**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**」で負荷分散グループに追加します。詳細については、『*SonicOS 6.5 システム設定* 管理ガイド』を参照してください。

プロビジョニング プロファイルの Bluetooth LE 設定

SonicWave シリーズは、標準的な Bluetooth のサブセットである Bluetooth 低消費電力 (BLE) 機能を備えています。BLE を使用すると、特に iBeacon 対応装置に非常に近接している場合、スマートフォン、タブレット、SonicWall モバイル アプリ、その他の SonicWaves などの他のデバイスを SonicWave アクセス ポイントに簡単に接続できます。BLE は位置推定も提供します。

iBeacon はアップルが開発したプロトコルです。さまざまなベンダーが、近くの携帯電子機器に識別子をブロードキャストする iBeacon 互換の BLE 機器を製造しています。このテクノロジにより、スマートフォン、タブレット、その他のデバイスは、iBeacon の近くにいるときにアクションを実行できます。

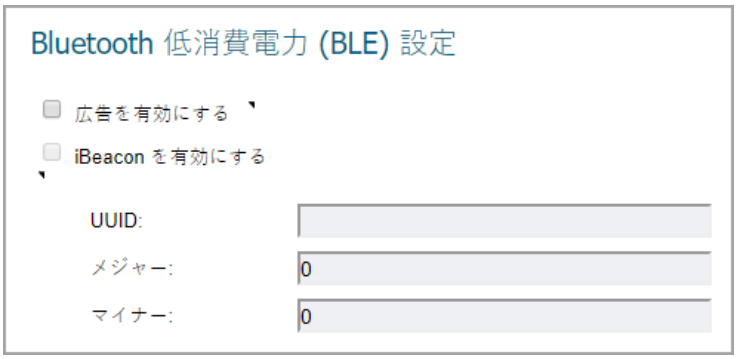
Bluetooth 低消費電力設定を有効にして設定するには:

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

2 「**SonicWave プロビジョニング プロファイル**」ボタンを選択します。

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

4 「**Bluetooth LE**」を選択します。



5 BLE 広告を有効にするには、「**広告を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。このオプションを有効にすると、「**iBeacon を有効にする**」オプションが使用可能になります。

> **メモ：**BLE アドバタイズメントを有効にすると、2.4G 無線周波数に影響または干渉する可能性があります。

6 BLE デバイスが識別子をブロードキャストするように iBeacon を有効にするには、「**iBeacon 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。従属するフィールドが使用可能になります。

7 フィールドに情報を入力します。

- **UUID** - UUID の 36 文字を入力します。以下に例を示します。

  `51b9d455-6a32-426c-b5cc-524181c24df3`

- **メジャー** - 同じ地理的グループで有効な ID を入力します。有効な範囲は 0 ～ 65535 で、既定値は **0** です。
- **マイナー** - 同じ地理的グループのセカンダリ ID を入力します。範囲は 0 から 65535 で、既定値は **0** です。

ヒント：異なる UUID を使用して異なる地理的グループを識別し、メジャーおよびマイナー オプションを使用して地理的グループ内の領域を識別します。例えば、1 つの建物に BLE を使用して複数の SonicWave 装置を展開し、これらの SonicWave 装置に同じ UUID を設定したとします。同じフロアの SonicWave 装置は、同じメジャー番号を持ちますが、同じフロアの異なる場所では異なるマイナー番号を持ちます。このように、お使いになっているモバイル機器の近くには SonicWave 装置があります。

8 「**OK**」を選択します。

アクセス ポイント プロファイルの削除

メモ：事前定義されているプロファイルは削除できません。削除できるのはユーザが追加したものだけです。

個々のプロファイルまたはプロファイルのグループの削除は、「**SonicPoint/SonicWave 接続 | アクセス ポイント > 基本設定**」ページの「**プロビジョニング プロファイル**」セクションで行えます。

- 1 つのアクセス ポイント プロファイルを削除するには、以下の手順に従ってください。
    1) 対応する「**削除**」ボタンを選択します。確認メッセージが表示されます。
    2) 「**OK**」を選択します。
- 1 つ以上の アクセス ポイント プロファイルを削除するには、以下の手順に従います。
    1) 削除する アクセス ポイント の名前の横にあるチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。
    2) 「**削除**」ボタンを選択します。確認メッセージが表示されます。
    3) 「**OK**」を選択します。
- すべてのプロファイルを削除するには、以下の手順に従います。
    1) 列見出しの **#** の横にあるチェックボックスをオンにします。「**すべての削除**」ボタンが使用可能になります。
    2) 「**すべて削除**」ボタンを選択します。確認メッセージが表示されます。
    3) 「**OK**」を選択します。

製品に特有の設定に関する注

SonicPoint 設定手順は、シングル無線 (SonicPointN) であるか、デュアル無線 (SonicWave、SonicPoint AC、およびSonicPoint NDR) 機器であるかによって若干異なります。

アクセス ポイントの管理

「**SonicPoint / SonicWave オブジェクト**」セクションには、接続されたアクセス ポイントの設定が表示されます。また、それらを編集したりその他のアクションを実行したりするためのボタンがあります。

このテーブルには、アクセス ポイントに設定された以下の値が表示されます。

列	説明
#	行参照番号
名前	アクセス ポイントの名前
インターフェース	アクセス ポイントが接続されているファイアウォール インターフェース番号とゾーン
ネットワーク設定	アクセス ポイントの IP アドレス、MAC アドレス、および管理指定
状況	動作中、応答なし、またはその他のアクセス ポイント状態
5GHz 無線	この無線、周波数、および 802.11 プロトコルのアクセス ポイント SSID (MSSID) 名
5GHz 無線チャンネル	帯域設定、チャンネル、および無線状態 (有効、アクティブなど)
2.4GHz 無線	この無線、周波数、および 802.11 プロトコルのアクセス ポイント SSID (MSSID) 名
2.4GHz 無線チャンネル	帯域設定、チャンネル、および無線状態 (有効、アクティブなど)
3G/4G/LTE	3G、4G、または LTE の有効/無効状態とバインディング情報
有効	アクセス ポイントが有効な場合に選択
設定	編集、削除、再起動、またはアクセス ポイントからログをダウンロードするためのボタン。手動キーセットを編集するためのボタンも表示できます。
SSH	アクセス ポイントへの SSH アクセス用のボタン

トピック:

- SonicPoint/SonicWave オブジェクトの削除
- SonicPoint/SonicWave オブジェクトの再起動
- SonicPoint/SonicWave オブジェクトの変更

SonicPoint/SonicWave オブジェクトの削除

個々の アクセス ポイントまたはアクセス ポイントのグループの削除は、「**SonicPoint/SonicWave 接続 | アクセス ポイント > 基本設定**」ページの「**オブジェクト**」セクションで行えます。

- 1 つのオブジェクトを削除するには、以下の手順に従います。
  a 対応する「**削除**」ボタンを選択します。確認メッセージが表示されます。
  b 「**OK**」を選択します。
- 1 つ以上のオブジェクトを削除するには、以下の手順に従います。
  a 削除するオブジェクトの横にあるチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。

b 「**削除**」ボタンを選択します。確認メッセージが表示されます。

c 「**OK**」を選択します。

- すべてのオブジェクトを削除するには、以下の手順に従います。
  a 列見出しの # の横にあるチェックボックスをオンにします。「**すべての削除**」ボタンが使用可能になります。
  b 「**すべて削除**」ボタンを選択します。確認メッセージが表示されます。
  c 「**OK**」を選択します。

SonicPoint/SonicWave オブジェクトの再起動

個々の アクセス ポイントまたはアクセス ポイントのグループの再起動は、「**接続 | アクセス ポイント > 基本設定**」ページの「**SonicPoint/SonicWave オブジェクト**」セクションで行えます。

- 1 つのオブジェクトを再起動するには、以下の手順に従います。
  a 再起動するアクセス ポイントの名前の横にあるチェックボックスをオンにします。「**再起動**」ボタンが使用可能になります。
  b 「**再起動**」ボタンを選択します。確認メッセージが表示されます。
  c 再起動の種別を選択します。
    - **再起動** (既定) - 設定したプロファイル設定で再起動します。
    - **工場出荷時の状態で再起動** - 工場出荷時の設定で再起動します。

△ **注意：このオプションを選択すると、アクセス ポイント プロファイルが工場出荷時の既定値で上書きされます。**

  d 「**OK**」を選択します。

- すべてのオブジェクトを再起動するには、以下の手順に従います。
  a 「**すべて再起動**」ボタンを選択します。
  b 次のいずれかを選択します。
    - **再起動** (既定) - 設定したプロファイル設定で再起動します。
    - **工場出荷時の状態で再起動**

△ **注意：このオプションを選択すると、アクセス ポイント プロファイルが工場出荷時の既定値で上書きされます。**

  c 「**OK**」を選択して適用してアクセス　ポイントを再起動するか、「**キャンセル**」を選択して再起動せずにウィンドウを閉じます。

SonicPoint/SonicWave オブジェクトの変更

アクセス ポイントの変更は、**接続 | アクセス ポイント > 基本設定**で行えます。

1 変更するオブジェクトの**編集**アイコンを選択します。
2 変更したい設定を変更します。
3 「**OK**」を選択して新しい設定を保存します。

メモ：ネットワーク装置が自動発見プロセスを実行すると、新しい SonicPoint/SonicWave アクセス ポイントが自動的に追加されます。

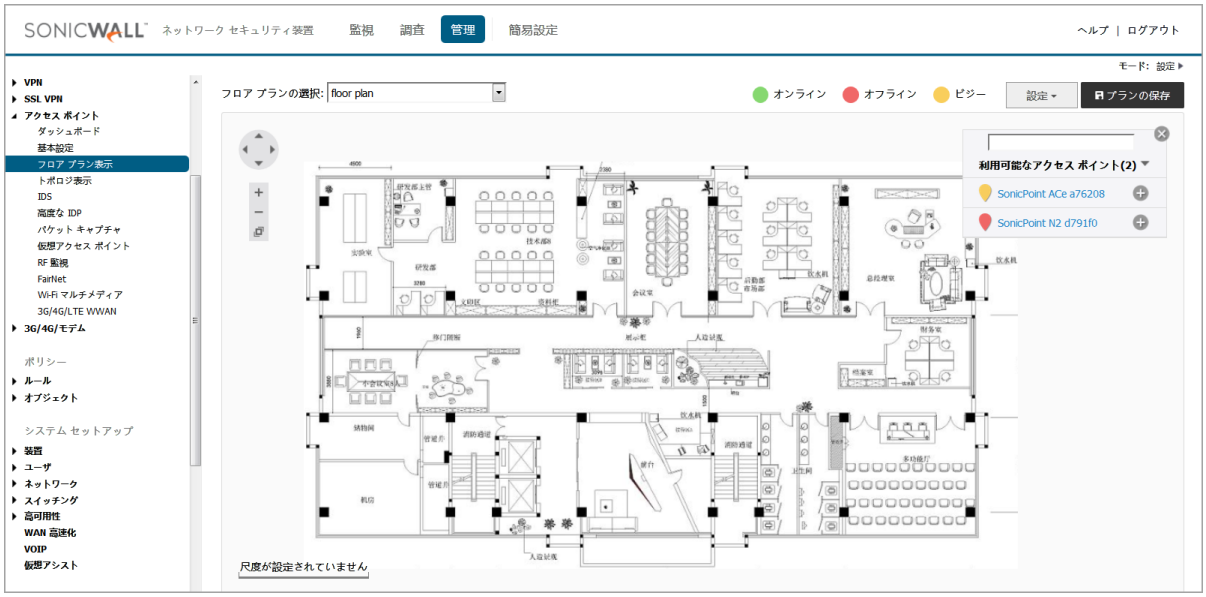
17

アクセス ポイント フロア プラン

「**管理**」表示の「**接続 | アクセス ポイント > フロア プラン表示**」ページで、SonicOS ユーザ インターフェースは多数の SonicWave と SonicPoint 機器を管理するためにより視覚的なアプローチを可能としています。また、物理的な位置とリアルタイムの状況も追跡できます。

フロア プラン表示は、既存の SonicOS 無線アクセス ポイント管理スイートに対するアドオンです。実際の無線配備環境をリアルタイムで図示し、新規の配備による無線通信範囲を推定するうえで役立ちます。FPMV はまた、コンテキスト メニューから、アクセス ポイント統計の確認、リアルタイムのアクセス ポイント状態監視、アクセス ポイント設定、アクセス ポイント除去、さらに RF 範囲の表示まで提供する、ワンストップのコンソールです。

次の図は、標準的なフロア プラン表示の例です。



トピック:

- フロア プランの管理
- アクセス ポイントの管理

フロア プランの管理

フロア プラン表示機能には、フロア プランを表示、追加、編集する多くの方法があります。このセクションでは、最も通常のものを説明します。

トピック:

- フロア プランの選択
- フロア プランの作成
- フロア プランの編集
- 測定用尺度の設定

フロア プランの選択

「**管理**」表示の「**接続 | アクセス ポイント > フロア プラン表示**」ページで、左上方の「**フロア プランの選択**」フィールドに、表示される フロア プランのタイトルが示されます。別のフロア プランを表示するには、「**フロア プランの選択**」ドロップダウン メニューから別のフロア プランを選択します。

フロア プランの選択の別の方法は以下のとおりです。

1 「**設定**」を選択します。

2 「フロア プラン リスト」を選択します。

3 表示したいプランの名前をダブルクリックします。

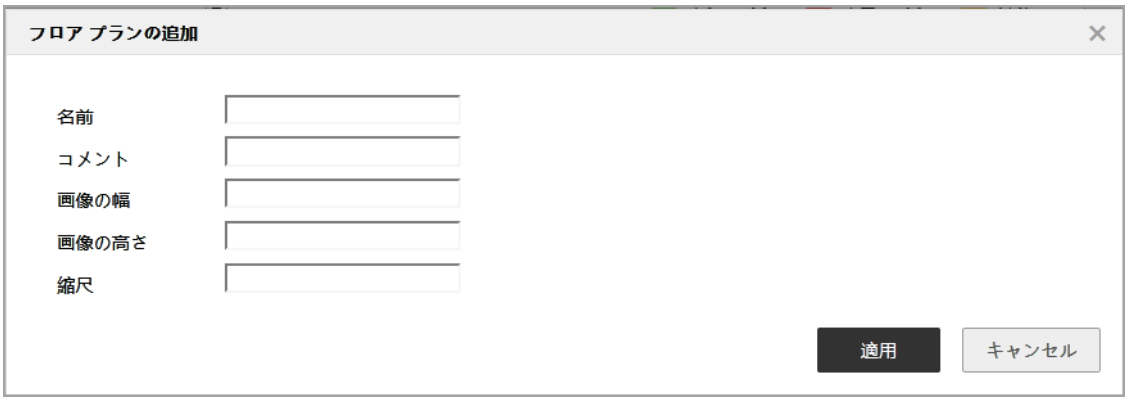
フロア プランの作成

フロア プランを作成するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。

2 「**設定**」を選択します。

3 「**フロア プランの追加**」を選択します。



4 プランを説明するフィールドに入力します。

5 「**適用**」を選択します。

フロア プランの編集

フロア プランの編集にはいくつかの方法があります。以下は最も通常の方法です。

表示中のフロア プランを編集するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。

2 「**設定**」を選択します。

3 「**現在のフロア プランの編集**」を選択します。

4 必要に応じてフィールドを変更します。

5 「**適用**」を選択します。

リスト上のプランを編集するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。

2 「**設定**」を選択します。

3 「**フロア プラン リスト**」を選択します。

4 **編集**アイコンを選択します。

5 必要に応じてフィールドを変更します。

6 「**適用**」を選択します。

測定用尺度の設定

実際の距離 (フィート) と、フロア プランの図を構成しているピクセルの関係を示すために、測定縮尺を設定する必要があります。この数値は、RF 範囲の推定の支援にも使用できます。

測定縮尺を設定するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。

2 「**設定**」を選択します。

3 「**測定縮尺の設定**」を選択します。ウィンドウに、**ラインの長**さフィールドが表示されます。

4 1 フィートあたりのピクセル数を入力します。

5 「**描画の終了**」をクリックします。

アクセス ポイントの管理

アクセス ポイントの状況が色で表示されます:

個々のアクセス ポイントが、**フロア プラン表示**で管理できます。

トピック:

- 利用可能なアクセス ポイント
- 追加されたアクセス ポイント
- アクセス ポイントの削除
- 画像としてエクスポート

利用可能なアクセス ポイント

配備に利用可能なアクセス ポイントが、「**利用可能なアクセス ポイント**」リストに表示されます。リストは通常右上隅に表示されますが、どこにでもドラッグ アンド ドロップできます。角にある「**x**」をクリックすると閉じることができます。「**設定 > 利用可能なアクセスポイント**」をクリックすると、リストが表示されます。

これらのアクセス ポイントをフロア プランにドラッグ アンド ドロップして、配備したい場所に置くことができます。作業が終わったら、必ず「**プランの保存**」を行ってください。

メモ：既にフロア プランに追加されているアクセス ポイントは、このパネルには表示されません。

追加されたアクセス ポイント

配備されたアクセス ポイントは、「**追加されたアクセス ポイント**」リストに表示されます。リストは通常右上隅に表示されますが、どこにでもドラッグ アンド ドロップできます。角にある「**x**」をクリックすると閉じることができます。「**設定 > 追加されたアクセス ポイント**」をクリックすると、リストが表示されます。

これらのアクセス ポイントをフロア プランにドラッグ アンド ドロップして、別の場所に置くことができます。また、プランから削除することもできます。作業が終わったら、必ず「**プランの保存**」を行ってください。

メモ：既にフロア プランに追加されているアクセス ポイントは、このパネルには表示されません。

アクセス ポイントの削除

すべてのアクセス ポイントを削除するには、以下の手順に従います。

1. 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。
2. 「**設定**」を選択します。
3. 「**すべての 追加されたアクセス ポイントの削除**」を選択します。
4. 「**プランの保存**」を選択します。

画像としてエクスポート

フロア プランの画像をエクスポートするには、以下の手順に従います。

1. 「**接続 | アクセス ポイント > フロア プラン表示**」に移動します。
2. 「**設定**」を選択します。
3. 「**画像としてエクスポート**」を選択します。
4. **JPG** 形式または **PNG** 形式のどちらで保存するかを選択します。
5. 後でアクセスできる場所に保存します。

コンテキスト メニュー

さまざまなコンテキスト メニューを動作させるために、マウスを利用できます。

- フロア プランのアクティブなアクセス ポイントの上にマウス ポインタを重ねると、ID、状況、クライアント数、稼働時間を含む、アクセス ポイント情報をポップアップ表示します。
- アクセス ポイントをクリックすると、RF 範囲が表示されます。
- アクセス ポイントをダブルクリックすると、リアルタイム監視ウィンドウが表示されます。
- アクセス ポイントを右クリックすると、コンテキスト メニューが表示されます。コンテキスト メニューは、編集、統計の表示、監視状況その他のオプションがあります。

18

アクセス ポイントのファームウェアの管理

「**管理 | 接続性 > アクセス ポイント > ファームウェアの管理**」ページでは、最新の SonicPoint/SonicWave ファームウェアを取得し、それでアクセス ポイントを更新できます。

トピック:

- ファームウェアの管理について
- 最新の SonicWall ファームウェアの入手
- 特定の URL からのファームウェアのダウンロード
- ファームウェアをアクセス ポイントにアップロードする

ファームウェアの管理について

「**ファームウェアの管理**」テーブルは、現在のアクセス ポイントのファームウェア イメージの状況を表示し、新しいファームウェアを取得してアクセス ポイントにアップロードするためのボタンを提供します。

列	説明
ファームウェア イメージ	ファームウェア イメージのアクセス ポイントの種別を表示します。
バージョン	アクセス ポイントで一致させる必要がある、ファイアウォールでサポートされているファームウェア バージョンを表示します。新しいバージョンの AP ファームウェアが提供されると、ファイアウォールがそれに対応していれば、「**バージョン**」項目に表示され、接続後にアクセス ポイントが新しいバージョンに自動的に更新されます。
状況	初期状態で、すべてのファームウェアの状況は、「*ダウンロードが必要*」となっています。別のファームウェア イメージがファイアウォール バッファにアップロードされると、*準備完了*を示すチェックマークに変わります。
ビルド日	アップロードされたファームウェアが作成された日付を表示します。
動作	次の 2 つのボタンを提供します。 • 「**ファームウェアのアップロード**」ボタン - ダウンロードされたファームウェアをファイアウォール バッファにアップロードします。上記の「**バージョン**」で説明したように、サポートされている新しい AP ファームウェアはアクセス ポイントに自動的にプッシュされます。ファームウェアを既に動作状態にあるアクセス ポイントにプッシュするには、内部設定を使用する必要があります。内部設定の使用については、SonicWall サポートにお問い合わせください。 • 「**ファームウェアのリセット**」ボタン - ダウンロードされたファームウェア イメージをバッファから削除します。

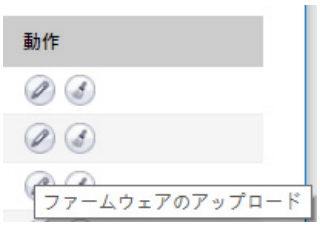
このページの「**ダウンロード URL**」セクションでは、HTTP を介して特定の場所から アクセス ポイント ファームウェア イメージをダウンロードすることができます。これにより、SonicWall サポートが提供する公式リリース前のバージョンなど、代替のファームウェアをロードできます。

最新の SonicWall ファームウェアの入手

SonicWall から最新版のファームウェアを入手するには:

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

2 「**ファームウェアの管理**」テーブルで、目的のアクセス ポイント種別の行の「**動作**」の下にある「**ファームウェアのアップロード**」ボタンを選択します。



3 「**ファームウェアのアップロード**」ダイアログボックスで、**software.sonicwall.com** リンクを選択します。

4 ポップアップ ダイアログで、「**ファイルの保存**」オプションを選択し、「**OK**」を選択ます。ファイルは、*Downloads* フォルダなどの既定の場所に保存されます。

5 ポップアップが閉じて、「**ファームウェアのアップロード**」ダイアログボックスに戻ります。

特定の URL からのファームウェアのダウンロード

URL の場所を手動で指定し、そこからファームウェア イメージをダウンロードしてアクセス ポイントで使用できます。

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 > ファームウェアの管理**」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 ダウンロードするイメージの種別を選択するチェックボックスをオンにします。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の URL を入力します。フィールドに "*http://*" を入力する必要はありません。

5 「**適用**」を選択します。ファイルはファイアウォール バッファに保存されます。

ファームウェアをアクセス ポイントにアップロードする

ローカルに保存されたファームウェア イメージ ファイルをアクセス ポイントにアップロードできます。保存されるファイルは、公式の SonicWall ファームウェア バージョン、または手動で指定した URL からダウンロードされたファームウェア イメージです。

ファームウェア イメージをアクセス ポイントにアップロードするには:

1 次のいずれかを実行して、ファームウェア イメージを取得し、ローカル ワークステーションに保存します。

- 「最新の SonicWall ファームウェアの入手」の説明に従って、公式の SonicWall バージョンをダウンロードします。

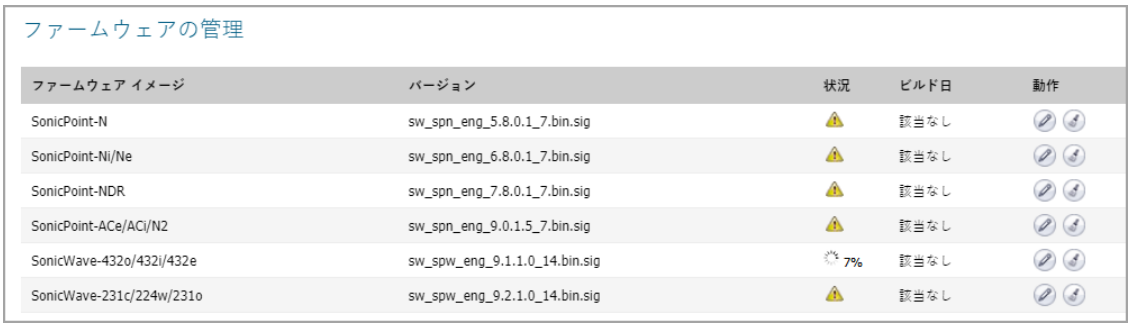
  この手順では、ローカル コンピュータにイメージ ファイルを保存した後、「**ファームウェアのアップロード**」ダイアログにとどまります。
- 「特定の URL からのファームウェアのダウンロード」の説明に従って、手動で指定した URL からファームウェア イメージをダウンロードします。

2 ファームウェア イメージをアップロードする場合は、目的のアクセス ポイント種別の行の「**動作**」の下にある「**ファームウェアのアップロード**」ボタンを選択して、「**ファームウェアのアップロード**」ダイアログ ボックスを開きます。**software.sonicwall.com** へのリンクを使用してイメージ ファイルをダウンロードした場合、ダイアログは既に開いています。

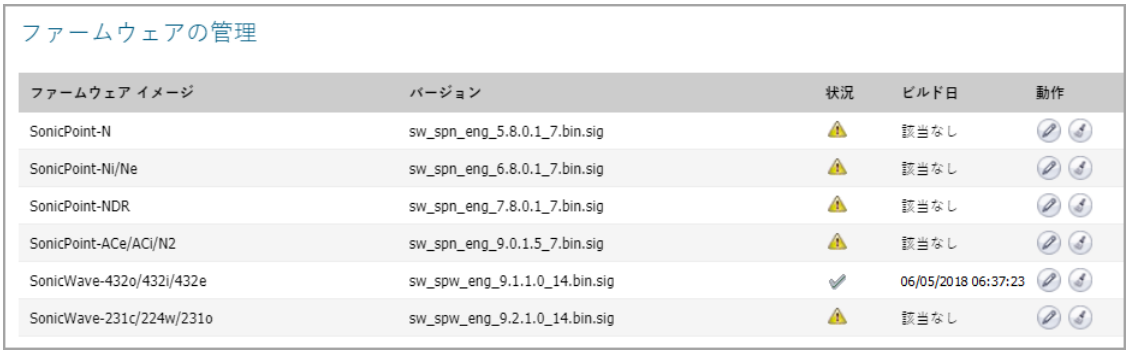
3 「**ファームウェアのアップロード**」ダイアログで、「**参照**」を選択し、保存されたイメージに移動して選択します。「**ファームウェアのアップロード**」ダイアログに、ファームウェア イメージ名が表示されるようになりました。

4 「**ファームウェアのアップロード**」ダイアログで、「**アップロード**」を選択します。

ファームウェア イメージは、セキュリティ装置のバッファにアップロードされます。アップロード中、「**状況**」にアップロードの割合が示されます。



アップロードが完了すると、「**バージョン**」列に新しいファームウェア バージョンが表示されます。アクセス ポイントが接続されている場合は、ファームウェア バージョンが自動的にプッシュされ、「**状況**」の表示がファームウェア イメージの*準備完了*を示すチェックマークに変わり、「**ビルド日**」にイメージの作成日付が表示されます。アクセス ポイントは現在、新しいファームウェアを実行しています。



5 ダウンロードしたファームウェアをバッファからクリアするには、「**動作**」の下の「**ファームウェアのリセット**」ボタンを選択します。「**状況**」インジケータと「**ビルド日**」は既定の表示に戻ります。

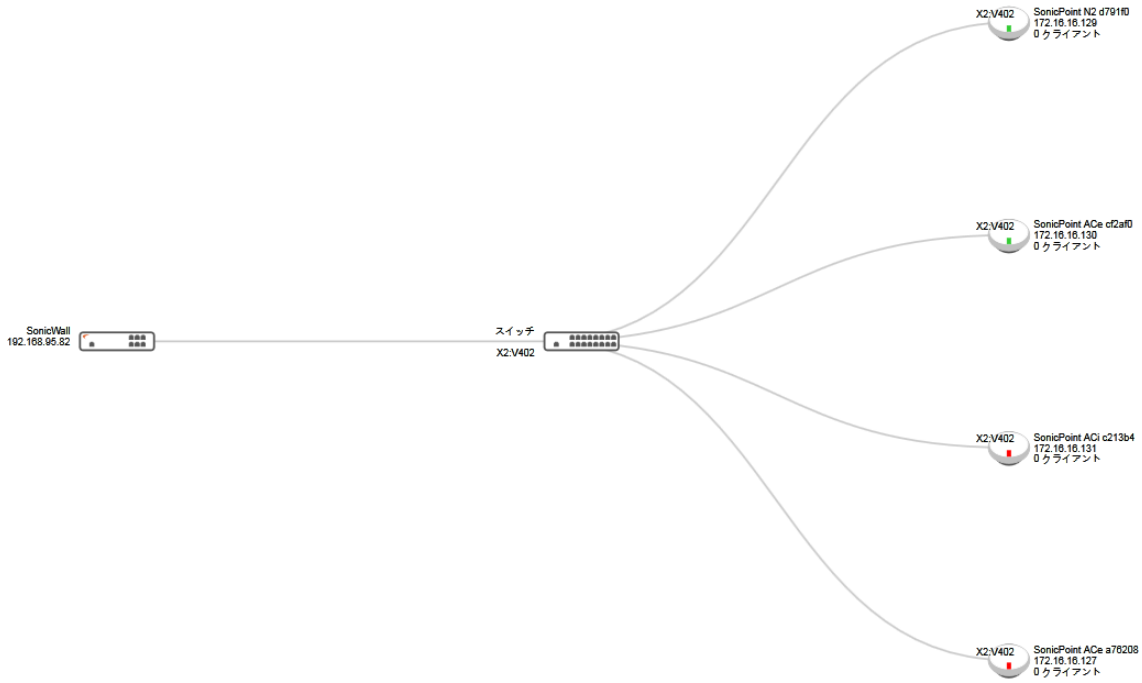
19

アクセス ポイント トポロジ表示

「**管理**」表示の「**接続 | アクセス ポイント > トポロジ表示**」ページで、アクセス ポイントを新しいトポロジ表示機能を使って管理できます。トポロジ表示は、SonicWall ファイアウォールから無線アクセス ポイントまでのネットワーク トポロジを表示します。アクセス ポイントのリアルタイムの状態を監視できます。コンテキスト メニューは、設定オプションも提供します。

この機能により、すべての WLAN ゾーンの機器間の論理的な関係を表示し、トポロジ表示で機器を直接管理できるようになります。

「**接続 | アクセス ポイント > トポロジ表示**」ページには、ファイアウォールが認識している機器をつなげ、それらの関係を示す、樹形または網目状の図が表示されます。以下の図と同様なものです。



トピック:

- トポロジ表示の管理
- トポロジ表示でのアクセス ポイントの管理

トポロジ表示の管理

トポロジ表示はシンプルなインターフェースです。表示を最新に維持し、インフラ内のアクセス ポイントを変更する手段を提供します。

トポロジが最新かどうかを確認したければ、いつでも、右下にある再検出ボタンをクリックしてください。こうすることで、装置に強制的に、無線インフラに何か変更が加わったかを確認させることができます。

トポロジ表示内で、個々の機器の詳細情報を得ることもできます。カーソルを機器の上に重ねると、ツールチップがポップアップします。機器の種別によって、名前、IP アドレス、インターフェース、モデルなどの情報を表示します。アクセス ポイントに対しては、状況やクライアント数など、追加情報が表示されます。

個々のアクセス ポイントは、状況を示すために色分けされています。

- 緑 = オンライン
- 赤 = オフライン
- 黄 = ビジー

トポロジ表示でのアクセス ポイントの管理

トポロジ表示にはコンテキスト メニューがあり、その中にはアクセス ポイントの管理に使用できる命令があります。

メモ：コンテキスト メニューはアクセス ポイントのみに適用されます。トポロジ マップ上の他の機器にはコンテキスト メニューはありません。

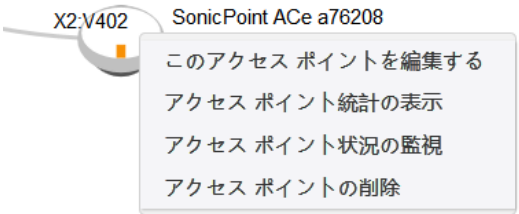
トピック:

- アクセス ポイントの編集
- 統計の表示
- アクセス ポイントの監視状況
- アクセス ポイントの削除

アクセス ポイントの編集

アクセス ポイントをトポロジ表示内で編集するには、以下の手順に従います。

1. 「**接続 | アクセス ポイント > トポロジ表示**」に移動します。
2. マウスを編集したいアクセス ポイントに重ねます。
3. アクセス ポイントを右クリックします。



4 「**このアクセス ポイントを編集する**」を選択します。

5 必要に応じて、オブジェクト設定に変更を加えます。

6 新しい設定を保存するために「**OK**」をクリックします。

統計の表示

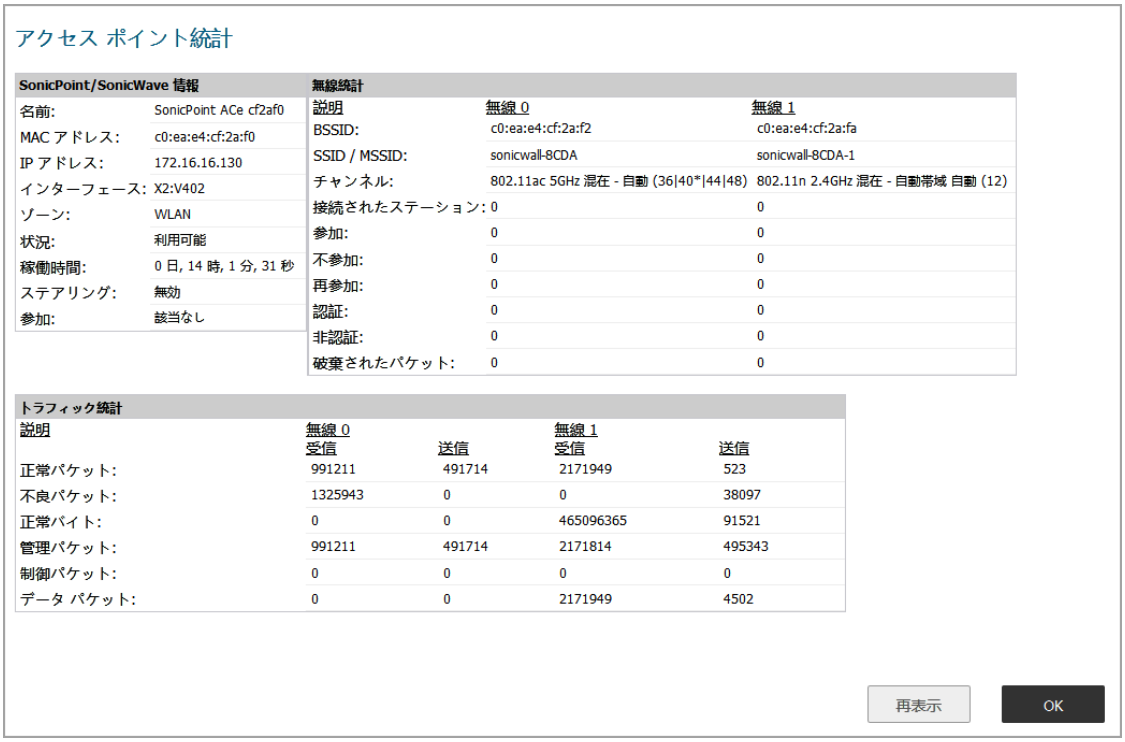
アクセス ポイントの統計を表示するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > トポロジ表示**」に移動します。

2 マウスを編集したいアクセス ポイントに重ねます。

3 アクセス ポイントを右クリックします。

4 「**アクセス ポイント統計**」の表示を選択します。



5 統計を再表示するには、「**再表示**」をクリックします。

6 完了したら「**OK**」を選択します。

アクセス ポイントの監視状況

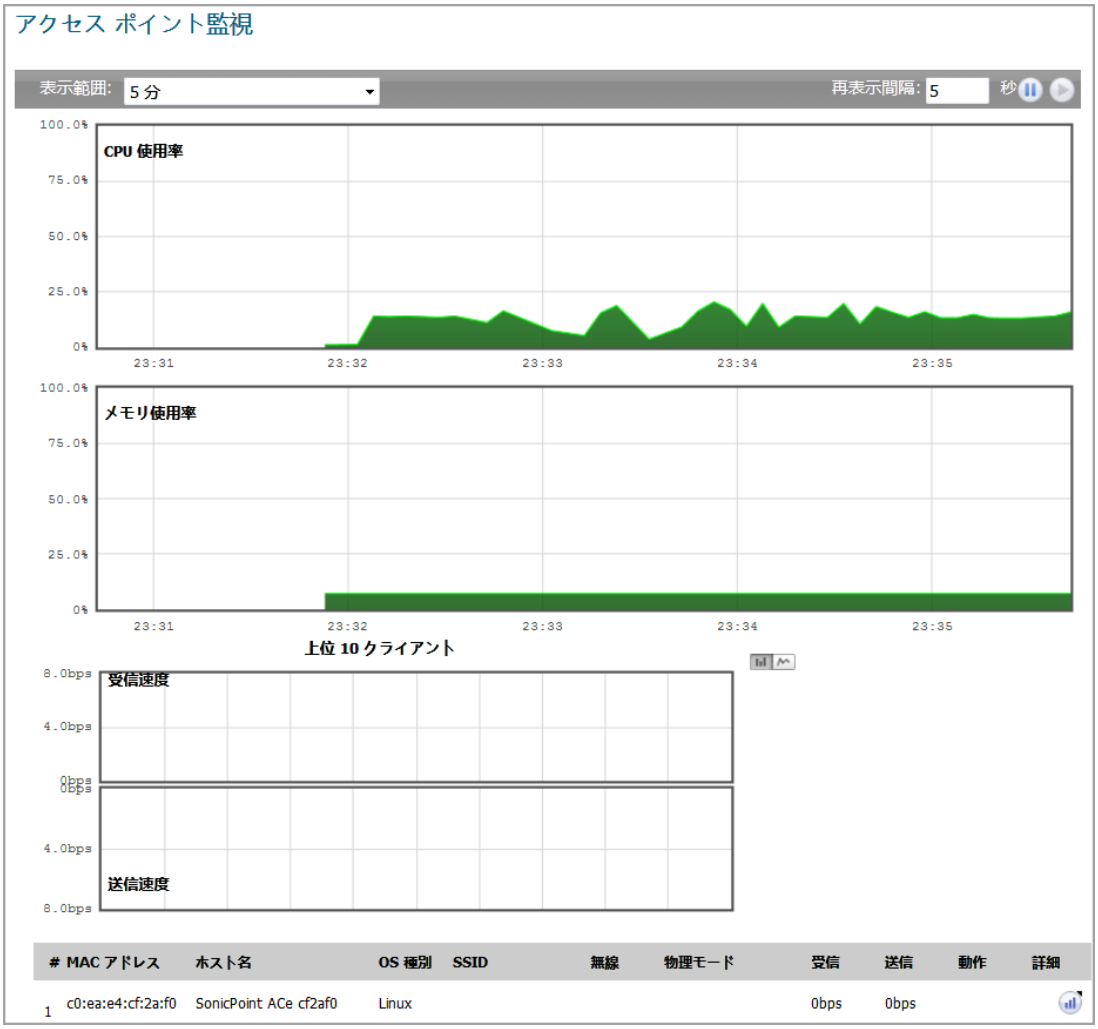
アクセス ポイントをトポロジ表示内で編集するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > トポロジ表示**」に移動します。

2 マウスを監視したいアクセス ポイントに重ねます。

3 アクセス ポイントを右クリックします。

4 「**アクセス ポイント監視状況**」を選択します。



アクセス ポイント監視は、アクセス ポイントの状況を表示します。CPU 使用率、メモリ使用率、受信速度と送信速度を含みます。

5 データを再表示するには、「**再表示**」をクリックします。

6 アクセス ポイントの詳細を表示するには、詳細アイコンをクリックします。

7 完了したら「**OK**」を選択します。

アクセス ポイントの削除

アクセス ポイントをトポロジ表示内で編集するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > トポロジ表示**」に移動します。

2 マウスを削除したいアクセス ポイントに重ねます。

3 アクセス ポイントを右クリックします。

4 「**アクセス ポイントの削除**」を選択します。

5 アクセス ポイントを削除する場合には確認を、そうでない場合にはキャンセルを行います。

20

アクセス ポイント侵入検知サービスの設定

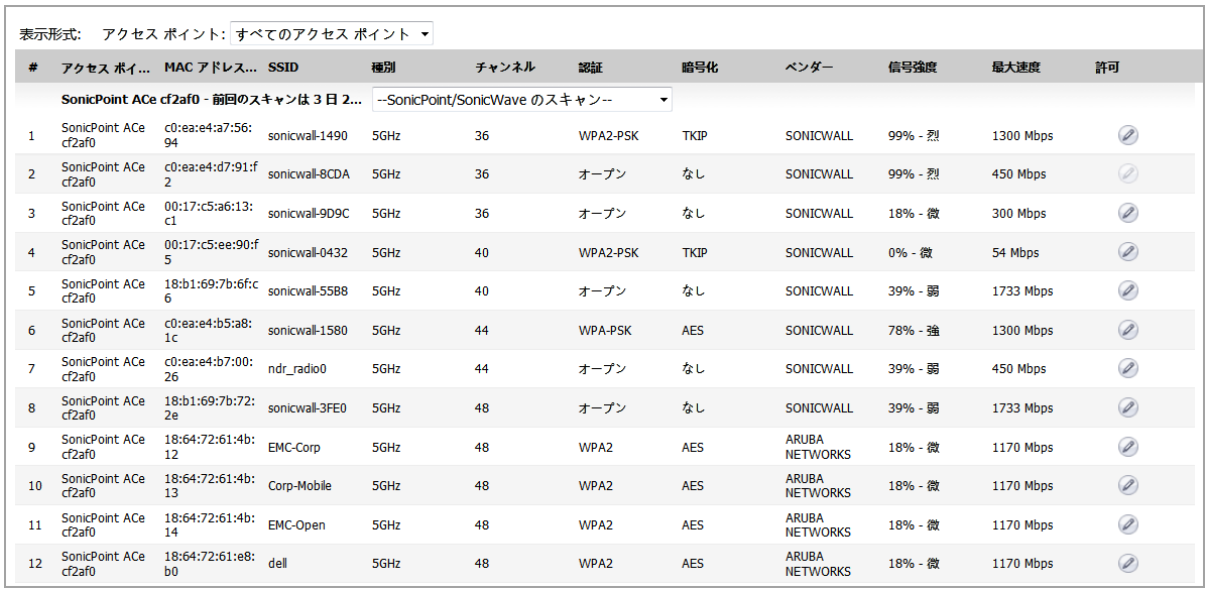
Rogue (悪意の侵入者) アクセス ポイントは、無線セキュリティに対する最も深刻かつ油断のならない脅威の 1 つです。一般に、ネットワーク上での使用が許可されていないアクセス ポイントは、悪意のあるアクセス ポイントとして認識されます。保護されていないアクセス ポイントの利便性や可用性と、ネットワークへの追加のしやすさによって、Rogue (悪意の侵入者) アクセス ポイントの導入を許す環境が形作られています。多種多様な脅威が生み出されています。

- 悪意のある機器への無意識的な接続
- 保護されていないチャンネルを介した機密データの転送
- LAN リソースへの不要なアクセス

これは特定の無線機器のセキュリティ不足ではなく、無線ネットワーク全体のセキュリティの脆弱性を示しています。

ファイアウォールでは、侵入検知サービス (IDS) によって、一般的な不正無線アクティビティの大半を認識して対応策を講じることができるようになり、そのセキュリティ機能が大幅に向上します。IDS は、802.11a、802.11g、および 802.11n 無線帯域をスキャンすることによって検出できるアクセス ポイントをすべて報告します。

「**管理**」表示の「**接続 | アクセス ポイント > IDS**」ページには、ファイアウォールとその関連アクセス ポイントによって検出される機器がすべて報告され、正当なアクセス ポイントを承認することができます。



表示形式: アクセス ポイント: すべてのアクセス ポイント

#	アクセス ポイ...	MAC アドレス...	SSID	種別	チャンネル	認証	暗号化	ベンダー	信号強度	最大速度	許可
	SonicPoint ACe cf2af0 - 前回のスキャンは 3 日 2...			--SonicPoint/SonicWave のスキャン--							
1	SonicPoint ACe cf2af0	c0:ea:e4:a7:56:94	sonicwall-1490	5GHz	36	WPA2-PSK	TKIP	SONICWALL	99% - 烈	1300 Mbps	
2	SonicPoint ACe cf2af0	c0:ea:e4:d7:91:f2	sonicwall-8CDA	5GHz	36	オープン	なし	SONICWALL	99% - 烈	450 Mbps	
3	SonicPoint ACe cf2af0	00:17:c5:a6:13:c1	sonicwall-9D9C	5GHz	36	オープン	なし	SONICWALL	18% - 微	300 Mbps	
4	SonicPoint ACe cf2af0	00:17:c5:ee:90:f5	sonicwall-0432	5GHz	40	WPA2-PSK	TKIP	SONICWALL	0% - 微	54 Mbps	
5	SonicPoint ACe cf2af0	18:b1:69:7b:6f:c6	sonicwall-55B8	5GHz	40	オープン	なし	SONICWALL	39% - 弱	1733 Mbps	
6	SonicPoint ACe cf2af0	c0:ea:e4:b5:a8:1c	sonicwall-1580	5GHz	44	WPA-PSK	AES	SONICWALL	78% - 強	1300 Mbps	
7	SonicPoint ACe cf2af0	c0:ea:e4:b7:00:26	ndr_radio0	5GHz	44	オープン	なし	SONICWALL	39% - 弱	450 Mbps	
8	SonicPoint ACe cf2af0	18:b1:69:7b:72:2e	sonicwall-3FE0	5GHz	48	オープン	なし	SONICWALL	39% - 弱	1733 Mbps	
9	SonicPoint ACe cf2af0	18:64:72:61:4b:12	EMC-Corp	5GHz	48	WPA2	AES	ARUBA NETWORKS	18% - 微	1170 Mbps	
10	SonicPoint ACe cf2af0	18:64:72:61:4b:13	Corp-Mobile	5GHz	48	WPA2	AES	ARUBA NETWORKS	18% - 微	1170 Mbps	
11	SonicPoint ACe cf2af0	18:64:72:61:4b:14	EMC-Open	5GHz	48	WPA2	AES	ARUBA NETWORKS	18% - 微	1170 Mbps	
12	SonicPoint ACe cf2af0	18:64:72:61:e8:b0	dell	5GHz	48	WPA2	AES	ARUBA NETWORKS	18% - 微	1170 Mbps	

次の表に、「**接続 | アクセス ポイント > IDS**」ページに表示される「**検出されたアクセス ポイント**」テーブルと項目を示します。

「検出されたアクセス ポイント」テーブルの構成要素

テーブルの列または項目	説明
項目	
「再表示」ボタン	画面を再表示して、ネットワーク内のアクセス ポイントの最新の一覧を表示します。
「すべてスキャン」ボタン	すべてのアクセス ポイントを呼び出し、接続された機器を特定する作業を開始する。
表示形式: アクセス ポイント	複数のアクセス ポイントがある場合は、「**アクセス ポイント**」ドロップダウン メニューで個々の機器を選択することも、また、すべてのアクセス ポイントが見たい場合は「**すべてのアクセス ポイント**」を選択することもできます。
「検出されたアクセス ポイント」テーブル	
アクセス ポイント	アクセス ポイント名は、「**すべての SonicPoint**」が **表示形式:** で選択されている場合にのみ表示されます。「**アクセス ポイント**」ドロップダウン メニュー
MAC アドレス (BSSID)	検出されたアクセス ポイントの無線インターフェースの MAC アドレスです
SSID	アクセス ポイントの無線 SSID です。
種別	機器によって使用される無線帯です。2.4GHz または 5GHz です。
チャンネル	アクセス ポイントで使用される無線チャンネルです。
認証	認証種別です
暗号化	暗号モードです
ベンダー	アクセスポイントのベンダーです。
信号強度	検出された無線信号の強度です。
最大速度	アクセス ポイントの無線で利用できる最高転送速度です。
許可	編集アイコンを選択すると、許可された機器のアドレス オブジェクト グループに機器が追加されます。

トピック:

- アクセス ポイントのスキャン
- アクセス ポイントの許可

アクセス ポイントのスキャン

アクティブ スキャンは、セキュリティ装置の起動時に実行されます。起動後にスキャンを命令した場合、無線クライアントの接続は数秒間切断されます。スキャンはトラフィックに次のように影響します。

- 非永続的で処理状態を把握しないプロトコル (HTTP など) には悪影響を及ぼしません。
- 永続的な接続 (FTP などのプロトコル) の場合は、接続状態が悪くなるか、切断されます。

- WiFiSec 接続は、クライアントが切断に気付かないように自動的に再確立され、再開される必要があります。

注意：すべてスキャン を選択すると、スキャン実行中に動作中の無線クライアントすべてが切断されます。サービスの中断が問題になる場合は、SonicWall セキュリティ装置がアクセス ポイント モードにある間はスキャンを命令しないことをお勧めします。アクティブなクライアントがなくなるまで、または一時的な切断であれば許容されるようになるまで待ちます。

スキャンを実行するには、以下の手順に従います。

1. 「**接続 | アクセス ポイント > IDS**」に移動します。
2. **表示形式:** で「**アクセス ポイント**」ドロップダウン メニュー (テーブルの最上部)で、すべての機器をスキャンするには「**すべてのアクセス ポイント**」を選択し、単一の機器をスキャンするには特定のアクセス ポイントを選択します。
3. テーブルの一番下には以下があります。
   - すべてのアクセス ポイントをスキャンする場合には、すべてをスキャンをクリックします。

     「**--アクセス ポイントのスキャンを実行--**」のドロップダウン メニューで、オプションを 1 つ選択できます。両方の無線のスキャン、「**無線 0 (5GHz) のスキャン**」または「**無線 1 (2.4GHz) のスキャン**」。
   - アクセス ポイントだけをスキャンするのであれば、「**--アクセス ポイントのスキャンを実行--**」のドロップダウン メニューで、オプションを 1 つ選択します。両方の無線のスキャン、「**無線 0 (5GHz) のスキャン**」または「**無線 1 (2.4GHz) のスキャン**」。

     メモ：1 つのアクセス ポイントだけを表示する場合、「**--アクセス ポイントのスキャンを実行--**」でテーブルの上部中央から右下に移動します。
4. スキャンを実行することを確認します。

アクセス ポイントの許可

セキュリティ装置によって検出されたアクセス ポイントは、その動作を許可するようにセキュリティ装置が設定されるまでは、Rogue (悪意の侵入者) とみなされます。

アクセス ポイントを許可するには、以下の手順に従います。

1. 「**接続 | アクセス ポイント > IDS**」に移動します。
2. 許可するアクセス ポイントの「**許可**」列にある**編集**アイコンを選択します。ポップアップが表示されます。

3. 「**OK**」を選択します。
4. アクセス ポイントの MAC アドレスが追加されたことを確認して、承認が成功したことを確認してください。詳細については、*SonicOS 6.5 システム設定*を参照してください。

21

高度な IDP を設定する

高度な侵入検知と防御 (IDP)、または無線侵入検知と防御 (WIDP) は、電波スペクトルを監視して、許可されていないアクセス ポイントの存在を検知 (侵入検知) し、管理者設定に基づいて自動的に防止策を実行 (侵入防御) します。アクセス ポイント上で高度な IDP を有効にすると、無線機能は専用の IDP センサーとして機能します。

注意：SonicWall アクセス ポイント無線で高度な IDP を有効にすると、アクセス ポイント機能は無効になり、すべての無線クライアントが切断されます。

SonicOS の無線侵入検知と防御は、SonicPoint と SonicWave アクセス ポイントに基づいており、SonicWall ゲートウェイと連係します。この機能は、これらのアクセス ポイントを、SonicWall ネットワークに接続している許可されていないアクセス ポイントを検知するための専用 WIDP センサーとして使用します。これには、KRACK Man-in-the-Middle アクセス ポイントの検知が含まれます。

注意：WIDP センサーとして設定された SonicPoint N は、アクセス ポイントとして機能できません。

アクセス ポイントが悪意のあるアクセス ポイントとして特定されると、その MAC アドレスが「すべての悪意のあるアクセス ポイント」アドレス オブジェクト グループに追加されます。

トピック:

- プロファイルで無線 IDP を有効にする
- 無線 IDP の設定
- KRACK スニッファ パケットの表示

プロファイルで無線 IDP を有効にする

スキャンのスケジュールを設定するなど、アクセス ポイント プロファイルで無線侵入検知と防御を有効にできます。アクセス ポイント プロファイルの詳細については、「プロビジョニング プロファイルの作成/変更」を参照してください。

アクセス ポイント プロファイルで高度な無線 IDP スキャンを有効にするには:

1. 「**接続 | アクセス ポイント>基本設定**」ページの「**SonicPoint/SonicWave プロビジョニング プロファイル**」に移動します。
2. 目的のインターフェースの**編集**アイコンを選択します。
3. **センサー** を選択します。

   ヒント：「センサー」画面は、すべての SonicPoint または SonicWave プロファイルで同じです。

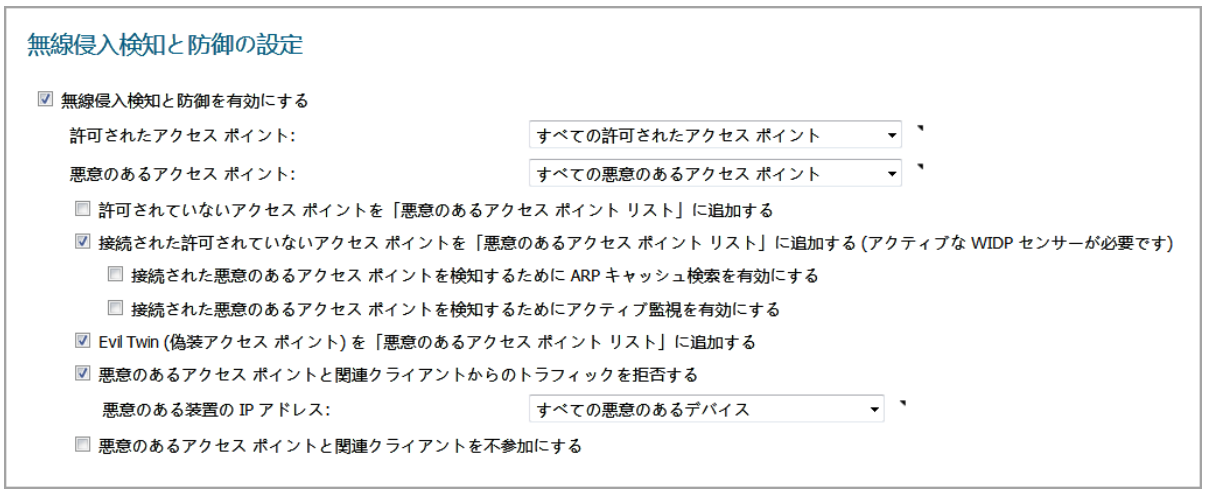
4. 「**WIDP センサーを有効にする**」を選択します。ドロップダウン メニューが使用可能になります。

5 ドロップダウン メニューから、IDP スキャンに対する適切なスケジュールを選択するか、「**スケジュールの作成**」を選択して個別スケジュールを作成します。

注意：SonicPoint/SonicWave 無線で高度な IDP スキャンを有効にすると、そのアクセス ポイント機能は無効になり、すべての無線クライアントが切断されます。

6 「**OK**」を選択します。

無線 IDP の設定



無線 IDP 設定を行うには:

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

2 「**無線侵入検知と防御を有効にする**」を選択して、装置による悪意のあるアクセス　ポイント (KRACK Man-in-the-Middle アクセス ポイントなど) の検索を有効にします。このオプションは既定では選択されていません。選択すると、その他のオプションがアクティブになります。

メモ：検出されたすべてのアクセス ポイントが、「**接続 | アクセス ポイント > IDS** 」ページの「**検出されたアクセス ポイント**」テーブルに表示され、許可する任意のアクセス ポイントを承認できます。

3 「**許可されたアクセス　ポイント**」に対して、許可されたアクセス　ポイントに割り当てるアドレス オブジェクト グループを選択します。既定では、これは「**すべての許可されたアクセス ポイント**」に設定されます。

メモ：SonicPoint N には、アクセス ポイント モードの仮想アクセス ポイント (VAP) は作成されません。ステーション モードの VAP が 1 つ作成され、IDS スキャンの実行、および保護されないアクセス ポイントへの接続とプローブ送信に使用されます。

4 「**悪意のあるアクセス ポイント**」に対して、許可されていないアクセス ポイントに割り当てるアドレス オブジェクト グループを選択します。既定では、これは「**すべての悪意のあるアクセス ポイント**」に設定されます。

5 どの AP を悪意があるか判別するための以下の 2 つのオプションから 1 つを選択します (同時に 2 つとも有効にすることはできません)。

- **「許可されていないアクセス ポイントを「悪意のあるアクセス ポイント リスト」に追加する」**は、検出されたすべての許可されていない AP を (それらがお使いのネットワークに接続しているかどうかにかかわらず)、自動的に Rogue リストに割り当てます。
- **「接続された許可されていないアクセス ポイントを「悪意のあるアクセス ポイント リスト」に追加する」**は、許可されていない AP がお使いのネットワークに接続している場合のみ、それらを Rogue リストに割り当てます。以下のオプションによって、IDP が接続された悪意のある AP を検出する方法が決まります。両方を選択することができます。
  - **接続された悪意のあるアクセス ポイントを検知するために ARP キャッシュ検索を有効にする** - 高度な IDP は、クライアント MAC アドレスを ARP キャッシュから検索します。それが発見されて、接続している AP が許可されていない場合に、その AP は悪意として分類されます。
  - **接続された悪意のあるアクセス ポイントを検知するためにアクティブ監視を有効にする** - SonicPoint/SonicWave が疑わしい AP に接続して、ファイアウォールのすべての LAN、DMZ、そして WLAN インターフェースにプローブを送信します。ファイアウォールがこれらのプローブのいずれかを受信した場合に、その AP は悪意として分類されます。

6 許可リストの中にはないが管理されているアクセス ポイントと同じ SSID を持つ機器を Rogue リストに追加するには、**「Evil Twin (偽装アクセス ポイント) を「悪意のあるアクセス ポイント リスト」に追加する」**を選択します。

7 Rogue リストと一致する送信元 IP アドレスを持つ受信トラフィックをすべて破棄するには、**「悪意のあるアクセス ポイントと関連クライアントからのトラフィックを拒否する」**を選択します。**「悪意のある装置の IP アドレス」**ドロップダウン メニューで、次のいずれかを実行します。

- **「すべての悪意のあるデバイス」**(既定)、または作成済みのアドレス オブジェクト グループを選択します。
- **「IP アドレス オブジェクト グループの作成」**を選択して、新しいアドレス オブジェクト グループを作成します。**「アドレス オブジェクト グループの追加」**ウィンドウが表示されます。

8 悪意のあるアクセス ポイントとの間の通信を停止するために、クライアントに認証解除メッセージを送信するには、**「悪意のあるアクセス ポイントと関連クライアントを不参加にする」**を選択します。

9 **「KRACK MITM AP との関連付けを解除してクライアントを不参加にする」**を選択して、KRACK 防御機能を有効にします。有効にすると、SonicWave は定期的に KRACK Man-in-the-Middle アクセス ポイントをチェックし、関連付けられているクライアントを検知すると、そのクライアントを KRACK MITM アクセス ポイントから積極的に切り離します。

10 **「適用」**ボタンを選択して変更を保存します。

KRACK スニッファ パケットの表示

「無線侵入検知と防御を有効にする」オプションが有効になっていると、SonicWave は無線環境を定期的にスキャンして KRACK Man-in-the-Middle アクセス ポイントおよびそれと情報を交換しているすべてのクライアントを検索します。***KRACK*** は、***Key Reinstallation Attack*** (鍵再インストール攻撃) の頭字語です。

KRACK MITM 攻撃は、実際のアクセス ポイントと同じ MAC アドレスを持つ別のチャンネルで実際のアクセス ポイントを複製します。KRACK MITM アクセス ポイントが検知されると、SonicWave は KRACK MITM と同じチャンネルで監視インターフェースを開き、チャンネル上のパケットを一定期間スニッ

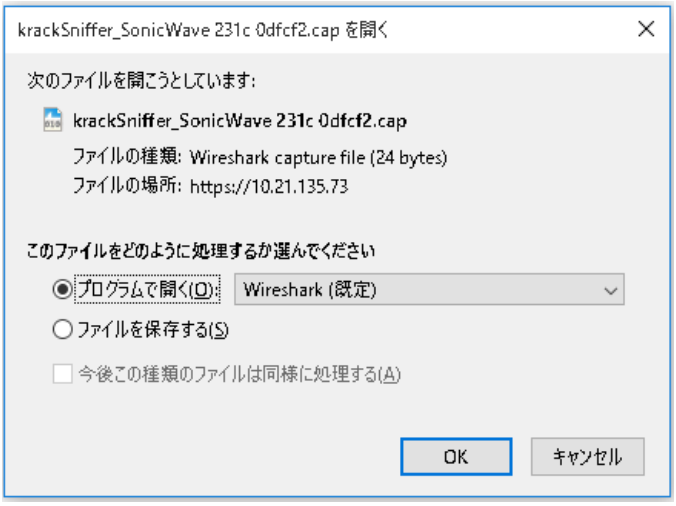
フィングします。MITM アクセス ポイントに関連付けられている無線クライアントがあり、「**KRACK MITM AP との関連付けを解除してクライアントを不参加にする**」オプションが有効になっている場合、そのクライアントは MITM アクセス ポイントから切り離されます。次のいずれかのイベントが発生すると、「**調査 | ログ > イベント ログ**」ページでログ メッセージが報告されます。

- KRACK MITM アクセス ポイントが検知された
- MITM アクセス ポイントと通信しているクライアントが検知された
- クライアントが MITM アクセス ポイントから切り離された

スニッフィングは KRACK 検知プロセス中に行われるため、キャプチャされたパケットは SonicWave のバッファに保存されます。「KRACK スニッファ統計」画像は、複数の SonicWave からの KRACK スニッファの結果を示しています。

KRACK スニッファ統計

KRACK プロセスを分析するには、SonicWave の「**ダウンロード**」ボタンを選択して、パケット データをファイル *krackSniffer_[SonicWave 名].cap* にエクスポートします。ここで *[SonicWave 名]* は SonicWave の名前です。次に、ファイルを開き、Wireshark または別の PCAP アナライザ ツールで調査します。



22

アクセス ポイントパケット キャプチャ

「**管理**」表示の「**接続 | アクセス ポイント > パケット キャプチャ**」機能は、クライアントから無線データを収集し、読解可能なファイルとして出力するために使用できる、詳しい無線トラブルシューティング種別を提供します。この機能は SonicWave アクセス ポイントでサポートされています。

メモ：スキャン無線のアンテナは 1 x 1 なので、一部のデータ フレームはハードウェアの制約によりスキャン無線でキャプチャできません。

「**アクセス ポイント > パケット キャプチャ**」ページのキャプチャ表示は、SonicWave の状況、キャプチャされたパケットの数、およびパケット バッファのサイズを表示します。右側にある「**設定**」列には、個々の SonicWave のキャプチャ設定を構築するためにクリックできるボタンが提供されています。

設定ダイアログでモード、帯域、およびチャンネルを設定し、特定のチャンネルの無線パケットをキャプチャすることができます。最大 5 個の送信元および送信先 MAC アドレスを設定できます。設定したい SonicWave の「**編集**」ボタンをクリックします。

設定した SonicWave 無線の 1 つについてデータをキャプチャするには、「**接続 | アクセス ポイント > パケット キャプチャ**」ページで、その無線の行の「**ダウンロード**」ボタンをクリックします。キャプチャ ファイルは、以下の形式の名前がつきます “wirelessCapture_[*SW 名*].cap”。ただし、*SW 名* は、SonicWave の名前です。ファイルの読み取りには Wireshark™ を使用できます。

23

仮想アクセス ポイントの設定

メモ：仮想アクセス ポイントは、SonicWall NSA 装置と共に無線アクセス ポイントを使う場合にサポートされます。

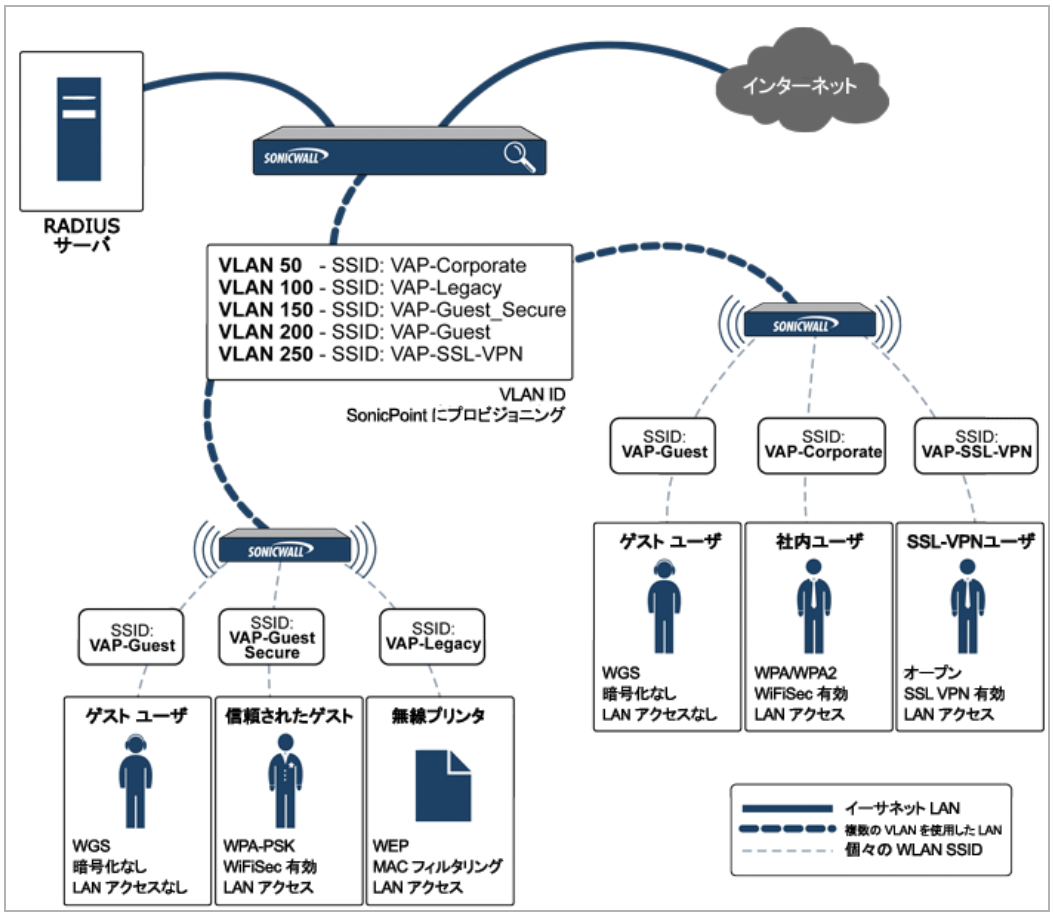
仮想アクセス ポイント (VAP) とは、単一の物理アクセス ポイントを多重インスタンス化したものです。それ自身を複数の別個なアクセス ポイントとして見せます。無線 LAN クライアントからは各仮想 AP が個別の物理 AP のように見えますが、実際には 1 つの物理 AP しか存在しません。VAP では、単一の物理インターフェース上で複数の個別設定をセットアップすることにより、無線ユーザ アクセスとセキュリティの設定を制御できます。これらの個別設定は、それぞれ別々の (仮想) アクセス ポイントとして機能し、またグループ化して、単一の内部ワイヤレス無線機に適用することができます。

SonicWall VAP 機能を使用すると、一意の基本サービス セット識別子 (BSSID) とサービス セット識別子 (SSID) が含まれるメディア アクセス コントロール (MAC) プロトコル レイヤの標準である IEEE 802.11 規格に準拠しています。そのため、単一の物理アクセス ポイント機器の単一の無線周波数フットプリント内で無線ネットワーク サービスをセグメント化できます。

VAP では、単一の物理インターフェース上で複数の個別設定をセットアップすることにより、無線ユーザ アクセスとセキュリティの設定を制御できます。これらの個別設定は、それぞれ別々の (仮想) アクセス ポイントとして機能し、またグループ化して、同時に単一または複数の物理アクセス ポイントに適用することができます。

トピック:

仮想アクセス ポイントの設定



VAP には次の利点があります。

- VAP ごとに個別のセキュリティ サービス設定 (GAV、IPS、CFS など) を持たせることができます。
- ゾーン レベルで設定したアクセス ルールを使って、各 VAP からのトラフィックを容易に制御できます。
- それぞれに別々のゲスト サービスまたはライトウェイト ホットスポット メッセージング (LHM) 設定を適用することができ、アクセス ポイントの共通セットで複数のゲスト サービス プロバイダの表示を容易にすることができます。
- 帯域幅管理やその他のアクセス ルール ベース制御を容易に適用することができます。

VAP を設定する前に

仮想アクセス ポイントを設定する前に、オプションにどのようなものがあり、何ができるのかを理解する必要があります。

トピック:

- VAP のニーズを確定する
- セキュリティ設定を確定する
- サンプル ネットワーク定義

- セキュリティ設定を確定する
- VAP 設定ワークシート

VAP のニーズを確定する

VAP の設定方法を決定するときは、まず以下のような通信ニーズについて検討してください。

- 何種類の無線ユーザをサポートする必要があるか。
- それらの無線ユーザをどのように保護するか。
- 選択したセキュリティ設定をサポートするために必要なハードウェアとドライバを無線クライアントが持っているか。
- 無線ユーザはどんなネットワーク リソースと通信する必要があるか。
- それらの無線ユーザの中に他の無線ユーザと通信する必要のあるユーザはいるか。
- それらの種類の無線ユーザの各々にどんなセキュリティ サービスを適用したいか。

セキュリティ設定を確定する

セキュリティの必要条件を理解したら、次にゾーン (およびインターフェース) と、ユーザに対して最も効果的に無線サービスを提供できる VAP を定義します。以下は、特定の種類のユーザを定義する方法の例です。

- **社内無線** - 信頼度の高い無線ゾーン。WPA2-AUTO-EAP セキュリティを使用します。WiFiSec (WPA) を執行します。
- **WEP & PSK** - 信頼度が中程度の無線ゾーン。これは 2 組の仮想 AP およびサブインターフェースで構成されます。1 つは旧式の WEP 機器 (無線プリンタ、旧式のハンドヘルド機器など) 用で、もう 1 つは WPA-PSK セキュリティを使用する来訪クライアント用です。
- **ゲスト サービス** - 内部ゲスト サービス ユーザ データベースを使用します。
- **LHM** - 外部 LHM 認証バックエンド サーバを使用するように設定したライトウェイト ホットスポット メッセージング対応ゾーン。

サンプル ネットワーク定義

以下のリストは、確実に適切なアクセスができるようにする前に、どのように仮想アクセス ポイントを設定するかの可能性のある方法の一例を示します。

- **VAP#1、社内無線ユーザ** - 普通はオフィスにいるユーザの集まりで、接続が認証されて安全であれば、すべてのネットワーク リソースへの完全なアクセスが許されるべき人たちです。これらのユーザはすでにネットワークのディレクトリ サービスである Microsoft アクティブ ディレクトリに属しています。 これはインターネット認証サービス (IAS) を通じて EAP インターフェースを提供します。
- **VAP#2、旧式の無線機器** - WEP 暗号化にしか対応していない旧式の無線機器の集まり (プリンタ、PDA、ハンドヘルド機器など)。
- **VAP#3、来訪パートナー** - オフィスを頻繁に訪れ、一部の信頼されたネットワーク リソースおよびインターネットにアクセスする必要のあるビジネス パートナー、クライアント、および関連会社の人たち。これらのユーザは会社のディレクトリ サービスに属していません。

- **VAP#4、ゲスト ユーザ** - インターネットなどの信頼されていないネットワーク リソースへのアクセスのみを許したい来訪クライアントです。一部のゲスト ユーザには、一時的で簡単なユーザ名とパスワードが与えられます。
- **VAP#5、頻繁なゲスト ユーザ** - ゲスト ユーザと同じですが、バックエンド データベースを通じて一時的でないゲスト アカウントが与えられます。

前提条件

仮想アクセス ポイントを設定する前に、以下に注意してください。

- 各 SonicWall アクセス ポイントが、仮想アクセス ポイントに対して明示的に有効にする必要があります。確認のため、「**接続 | アクセス ポイント > 基本設定**」に移動します。「**SonicPoint/SonicWave プロビジョニング プロファイル > 一般設定**」の**編集**アイコンを選択します。「**SonicPoint/SonicWave を有効にする**」チェックボックスを選択し、無線 A または G のいずれかを有効にします。
- アクセス ポイントのプロビジョニングが行われるようにするには、アクセス ポイントを SonicWall ネットワーク セキュリティ装置上の WLAN ゾーンにリンクする必要があります。
- VAP と共に VLAN を使用するときは、物理アクセス ポイントの検出パケットと配布パケットにタグ付けされないようにする必要があります (ファイアウォール上の VLAN サブインターフェースを終端とするのでない限り)。
- アクセス ポイントによって VLAN タグが付けられた VAP パケットが、ネットワーク上の中間機器 (VLAN 対応のスイッチなど) によって変更されずに (カプセル化解除も二重カプセル化も行われずに) 配信されるようにする必要もあります。
- 最大アクセス ポイント制限は SonicWall セキュリティ装置に応じて適用され異なります。

VAP 設定ワークシート

「VAP 設定ワークシート」テーブル は、VAP 設定に関する一般的な検討事項とソリューション、および実際の設定内容を記入するための空欄から成っています。

VAP 設定ワークシート

質問	例	ソリューション
どれだけの種類の無線ユーザをサポートする必要があるか。	社内無線、ゲスト アクセス、来訪パートナー、無線機器は、すべて一般的なユーザ種別で、それぞれ固有の VAP を必要とする。	異なる VAP の必要数を把握します。必要な各 VAP についてゾーンとVLAN を設定します。
	実際の設定内容:	

VAP 設定ワークシート

質問	例	ソリューション
各 VAP でどれだけのユーザをサポートする必要があるか。	会社の構内に 100 人の従業員がいて、全員が無線機能を使用する。	少なくとも 100 個のアドレスを提供するように訪問者ゾーンの DHCP スコープを設定します。
	会社の構内に無線機能を使用できる 20〜30 人の訪問者がよく来訪する。	少なくとも 25 個のアドレスを提供するように訪問者ゾーンの DHCP スコープを設定します。
	実際の設定内容:	
異なる種類の無線ユーザをどのように保護するか。	社内 LAN リソースにアクセスできる社内ユーザ。	WPA2-EAP を設定します。
	インターネット アクセスのみに限定されたゲスト ユーザ。	ゲスト サービスを有効にしますが、セキュリティ設定は行いません。
	社内 LAN 上の旧式の無線プリンタ。	WEP を設定し、MAC アドレス フィルタを有効にします。
	実際の設定内容:	
ユーザはどんなネットワーク リソースと通信する必要があるか。	社内 LAN とすべての内部 LAN リソース (他の WLAN ユーザも含む) へのアクセスを必要とする社内ユーザ。	社内ゾーンに関してインターフェース間通信を有効にします。
	インターネット アクセスを必要とするが、他の WLAN ユーザとの通信は許可すべきでない無線ゲスト。	ゲスト ゾーンに関してインターフェース間通信を無効にします。
	実際の設定内容:	
ユーザにどんなセキュリティ サービスを適用したいか。	完全な SonicWall セキュリティ スイートで保護すべき社内ユーザ。	SonicWall のすべてのセキュリティ サービスを有効にします。
	社内 LAN 上にいないので、配慮する必要のないゲスト ユーザ。	SonicWall のすべてのセキュリティ サービスを無効にします。
	実際の設定内容:	

アクセス ポイントVAP設定 タスク リスト

アクセス ポイント VAP を配備するには、いくつかの設定手順を実行する必要があります。このセクションでは、関連するステップの概要を説明します。

1 **ネットワーク ゾーン** - ゾーンは VAP 設定の重要部分です。作成した各ゾーンは、それぞれに個別のセキュリティ設定とアクセス制御設定を持つことになります。複数のゾーンを作成し、VLAN サブインターフェースを通じて単一の物理インターフェースに適用することができます。ネットワーク ゾーンの詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > ゾーン**」のセクションを参照してください。

2 **インターフェース (または VLAN サブインターフェース)** - インターフェース (X2、X3 など) は SonicWall ネットワーク セキュリティ装置と物理アクセス ポイントの間の物理接続を表します。個々のゾーン設定はこれらのインターフェースに適用され、それからアクセス ポイントに転送されます。無線インターフェースの詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > インターフェース**」のセクションを参照してください。

3 **DHCP サーバ** - DHCP サーバはリースされる IP アドレスを指定された範囲 (「*スコープ*」と呼ばれる) 内のユーザに割り当てます。DHCP スコープの既定の範囲は、たいていの SonicPoint 配備のニーズにとって過大なものです (例えば、30 個のアドレスしか使用しないインターフェースに対して 200 個のアドレスというスコープ)。そのため、利用可能なリース スコープを使い果たさないように、DHCP 範囲は気をつけて設定する必要があります。DHCP サーバ設定の詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > DHCP サーバ**」のセクションを参照してください。

4 **仮想アクセス ポイント プロファイル** - **仮想アクセス ポイント プロファイル** 機能では、必要に応じて新しい無線仮想アクセス ポイントに簡単に適用できる無線設定プロファイルを作成できます。詳細については、「**仮想アクセス ポイント プロファイル**」を参照してください。

5 **仮想アクセス ポイント オブジェクト** - **仮想アクセス ポイント オブジェクト** 機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および VLAN ID が設定されます。詳細については、「**仮想アクセス ポイント**」を参照してください。

6 **仮想アクセス ポイント グループ** - **仮想アクセス ポイント グループ** 機能では、単一のアクセス ポイントに同時に適用する複数の仮想アクセス ポイント オブジェクトをグループ化することができます。

7 **仮想アクセス ポイント グループをアクセス ポイント プロファイル無線に割り当てる** - プロビジョニング プロファイルでは、新しいアクセス ポイントのプロビジョニング時に VAP グループを適用できます。

8 **WEP 鍵を割り当てる (WEP 暗号化のみ)** - WEP 鍵の割り当てでは、新しいアクセス ポイントのプロビジョニング時に WEP 暗号化鍵を適用できます。WEP 鍵はアクセス ポイントごとに設定されます。つまりアクセス ポイントに割り当てられた WEP 対応の仮想アクセス ポイントは、すべて同じセットの WEP 鍵を使用しなければなりません。4 つまでの鍵を定義できます。 WEP 対応の VAP は、この 4 つの鍵を独立に使用できます。WEP 鍵の設定は「**設定 | アクセス ポイント > 基本設定**」ページで アクセス ポイント プロファイルまたは個々のアクセス ポイントに対して行います。

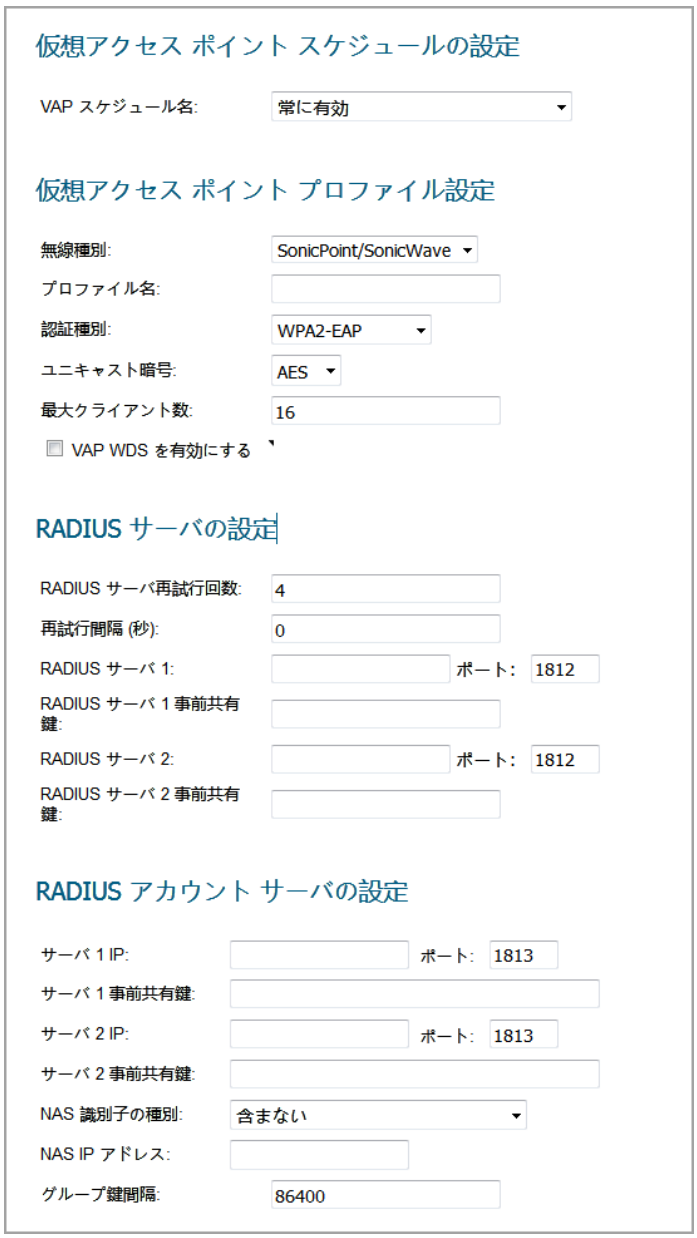
仮想アクセス ポイント プロファイル

仮想アクセス ポイント プロファイルを使用すると、アクセス ポイント設定をあらかじめ設定して、プロファイルに保存することができます。仮想アクセス ポイント プロファイルにより、新しい仮想

アクセス ポイントに簡単に設定を適用することができます。仮想アクセス ポイント プロファイルの設定は「**接続 | アクセス ポイント > 仮想アクセス ポイント** ページの **仮想アクセス ポイント プロファイル**」で行います。

既存の VAP プロファイルを設定するには、そのプロファイルに対する**編集**アイコンを選択します。「**追加**」ボタンを選択して、新しい VAP プロファイルを追加します。

メモ：表示されるオプションは、他のオプションの選択内容によって変わります。



トピック:

- 仮想アクセス ポイント スケジュールの設定
- 仮想アクセス ポイント プロファイルの設定
- ACL 強制
- リモート MAC アドレス アクセス制御の設定

仮想アクセス ポイント スケジュールの設定

個々の仮想アクセス ポイントは固有のスケジュールを持つことができます。拡張により、個々のプロファイルも専用に定義されたスケジュール設定を持つことができます。

スケジュールを仮想アクセス ポイント プロファイルに関連付けるには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**アクセス ポイント > 仮想アクセス ポイント**」を選択します。

3 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して**編集**アイコンをクリックします。

4 「**VAP スケジュール名**」フィールドで、スケジュールをドロップダウン メニューから選択します。

仮想アクセス ポイント プロファイルの設定

仮想アクセス ポイント プロファイルを設定するには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して**編集**アイコンをクリックします。

4 「**無線種別**」を設定します。アクセス ポイントを仮想アクセス ポイントとして使用する場合、「**SonicPoint/SonicWave**」に設定します。(現在のところサポートされる唯一の無線種別です)

5 「**プロファイル名**」フィールドに、この仮想アクセス ポイント プロファイルのわかりやすい名前を入力します。後でこのプロファイルを新しい VAP に適用するときにわかりやすく、覚えやすい名前にするとよいでしょう。

6 「**認証種別**」をドロップダウン リストから選択します。以下のオプションから選択します。

認証種別	定義
オープン	認証方法を特定しない。安全でないアクセスです。
共有	共有鍵が認証に使用され、基本的なセキュリティが確保されます。
両方	保護されない共有アクセス。

認証種別	定義
WPA2-PSK	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。認証に事前共有鍵を使います。
WPA2-EAP	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。拡張認証プロトコル (EAP) を使用します。
WPA2 - 自動 - PSK	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。認証には事前共有鍵を使用します。
WPA2 - 自動 - EAP	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。拡張認証プロトコル (EAP) を使用します。

選択された認証種別に基づいて、「**ユニキャスト暗号**」フィールドが表示されます。

メモ：ページに表示される設定は、選択したオプションに応じて異なります。

選択された「**認証種別**」に応じて、仮想 アクセス ポイント プロファイルの追加/編集ページには、追加のオプションのセクションが表示されます。

- オープンを選択した場合、RADIUS 設定については「RADIUS サーバと RADIUS アカウント」を参照してください。
- 「**両方**」または「**共有**」を選択した場合の設定の情報については、「WEP 暗号化の設定」を参照してください。
- 事前共有鍵 (PSK) を必要とするオプションを選択した場合の設定の情報については、「WPA-PSK > WPA2-PSK 暗号化の設定」を参照してください。
- 拡張認証プロトコル (EAP) を使用するオプションを選択した場合の設定の情報については、「RADIUS サーバと RADIUS アカウント」を参照してください。

WEP 暗号化の設定

前の手順のステップ 6 で「**両方**」または「**共有**」を選択した場合、「**WEP 暗号化設定**」と呼ばれる設定が表示されます。WEP 設定は、物理アクセス ポイントを共有する仮想アクセス ポイント間で共有されます。

暗号化を設定するには、以下の手順に従います。

1 「**暗号化鍵**」フィールドで、「**第 1 鍵**」、「**第 2 鍵**」、「**第 3 鍵**」、または「**第 4 鍵**」をドロップダウン リストから選択します。

2 リモート MAC アクセス制御を有効にしている場合は、RADIUS をセットアップするために、「RADIUS サーバと RADIUS アカウント」に移動してください。

WPA-PSK > WPA2-PSK 暗号化の設定

ステップ 6 で、事前共有鍵が必要なオプション - 「**WPA2-PSK**」または「**WPA2-AUTO-PSK**」 - を選択した場合、「**WPA/WPA2-PSK 暗号化設定**」と呼ばれる設定が表示されます。これらの設定が定義されると、事前共有鍵が認証に使用されます。

暗号化を設定するには、以下の手順に従います。

1 「**パス フレーズ**」フィールドにパスワードを入力します。

2 リモート MAC アクセス制御を有効にしている場合は、RADIUS をセットアップするために、「RADIUS サーバと RADIUS アカウント」に移動してください。

RADIUS サーバと RADIUS アカウント

ステップ 6 で選択したすべての設定に対して、RADIUS サーバを設定することができます。この設定が定義されると、鍵の生成および認証に外部の 802.1x/EAP 対応 RADIUS サーバを利用します。以下のフィールドに値を入力します。

RADIUS サーバの設定を行うには、以下の手順に従います。

フィールド名	説明
RADIUS サーバ再試行回数	アクセスを拒否するまでにユーザが認証を試行できる回数を入力します。既定値は 4 です。
再試行間隔 (秒)	再試行が有効な期間を入力します。既定値は 0 です。
RADIUS サーバ 1	RADIUS 認証サーバの名前/場所を入力します。
ポート	プライマリ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポートを入力します。
RADIUS サーバ 1 事前共有鍵	プライマリ RADIUS サーバ用のシークレット パスコードを入力します。
RADIUS サーバ 2	バックアップ RADIUS 認証サーバの名前/場所を入力します。
ポート	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポートを入力します。
RADIUS サーバ 2 事前共有鍵	バックアップ RADIUS 認証サーバ用のシークレット パスコードを入力します。

RADIUS アカウント サーバの設定を行うには、以下の手順に従います。

いいえ

フィールド名	説明
サーバ 1 IP	プライマリ RADIUS サーバの IP アドレスを入力します。
ポート	プライマリ RADIUS アカウント サーバがクライアントおよびネットワーク機器と通信するポートを入力します。
サーバ 1 事前共有鍵	プライマリ RADIUS アカウント サーバ用のシークレット パスコードを入力します。
サーバ 2 IP	バックアップ RADIUS サーバの IP アドレスを入力します。
ポート	バックアップ RADIUS アカウント サーバがクライアントおよびネットワーク機器と通信するポートを入力します。

フィールド名	説明
サーバ 2 事前共有鍵	バックアップ RADIUS アカウント サーバ用のシークレット パスコードを入力します。
NAS 識別子の種別	ドロップダウン メニューから NAS 識別子種別 を選択します。オプションは以下を含みます。含まない (既定)、アクセス ポイント名、アクセス ポイント MAC アドレス、SSID。 「SSID」オプションが選択されている場合、RADIUS 認証メッセージと RADIUS アカウント メッセージの両方で VAP SSID が伝送されます。
NAS IP アドレス	NAS システムの IP アドレスを入力します。
グループ鍵間隔	グループ鍵の有効時間を秒単位で入力します。この時間が経過すると、グループ鍵が強制的に更新されます。既定値は **86400** 秒です。(24 時間)

ACL 強制

各仮想アクセス ポイントは、個別のアクセス制御リスト (ACL) をサポートして、より効率的な認証制御を提供できます。この無線 ACL 拡張機能は、現在 SonicOS で利用可能な無線 MAC フィルタ リストと同時に動作します。この ACL 強制機能を使って、ユーザは MAC フィルタ リストを有効/無効にする、許可リストを設定する、そして拒否リストを設定することが可能です。

各 VAP は個別の MAC フィルタ リスト設定を持つ、またはグローバル設定を使うことが可能です。グローバル設定が有効な場合は、SonicWave、SonicPoint-N/ SonicPointNDR/ SonicPoint Ni/Ne、SonicPoint 装置は既定でこれらの設定を使います。仮想アクセス ポイント (VAP) モードでは、このグループの各 VAP が同一 MAC フィルタ リスト設定を共有します。

ACL 強制の設定

オプション	説明
MAC フィルタ リストを有効にする	特定の機器からのトラフィックを許可または禁止することによって、アクセス制御を行います。既定では、このオプションは選択されておらず、このセクションのすべてのオプションがグレー表示で利用できない状態になっています。
グローバル ACL 設定を使用する	グローバル ACL 設定を使用します。 **メモ**：仮想アクセス ポイントごとの ACL サポートは、SonicPointN によってのみサポートされています。1 つの仮想アクセス ポイントが SonicPoint/SonicWave によって使用されている場合、グローバルな ACL 設定が既定で適用されます。

ACL 強制の設定

オプション	説明
許可リスト	MAC アドレス グループを選択すると、そのグループ内の MAC アドレスを持つすべての機器からのトラフィックが自動的に許可されます。 • **新しい MAC アドレス オブジェクト グループの作成** • **すべての MAC アドレス** **メモ：「許可リスト」**には**「すべての MAC アドレス」**を設定することを推奨します。 • **既定の SonicPoint/SonicWave ACL 許可グループ** • ユーザ定義の MAC アドレス オブジェクト グループ
拒否リスト	ドロップダウン メニューから MAC アドレス グループを選択すると、そのグループ内の MAC アドレスを持つすべての機器からのトラフィックが自動的に拒否されます。 **メモ：拒否リスト**が適用された後で、**許可リスト**が適用されます。 • **新しい MAC アドレス オブジェクト グループの作成** • **MAC アドレスなし** • **既定の SonicPoint/SonicWave ACL 拒否グループ** **メモ：「拒否リスト」**には**「既定の SonicPoint/SonicWave ACL 拒否グループ」**を設定することを推奨します。 • ユーザ定義の MAC アドレス オブジェクト グループ

リモート MAC アドレス アクセス制御の設定

メモ：このセクションは、**「認証種別」**として**「WPA2/WPA2-自動-EAP」**が選択されている場合は表示されません。

リモート MAC アドレス アクセス制御の設定

オプション	説明
リモート MAC アクセス制御を有効にする	リモート RADIUS サーバにおける、MAC ベースの認証ポリシーに基づく無線アクセス制御を強制する場合、このチェックボックスをオンにします。既定では、このオプションはオフになっています。 **メモ：「認証種別」**として**「WPA2/WPA2-自動-EAP」**以外を選択した場合は、**「リモート MAC アクセス制御を有効にする」**を選択すると、**「RADIUS サーバの設定」**セクションが表示されます。

仮想アクセス ポイント

VAP 設定機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および VLAN ID が設定されます。仮想アクセス ポイントの設定は**「アクセス ポイント > 仮想アクセス ポイント」**ページで行います。

既存の VAP を設定するには、その VAP に対する「**編集**」アイコンを選択します。「**追加**」ボタンを選択して、新しい VAP を追加します。

トピック:

- 一般パネル (255 ページ)
- 詳細タブ (256 ページ)

一般パネル

一般パネルの以下の機能を設定します。

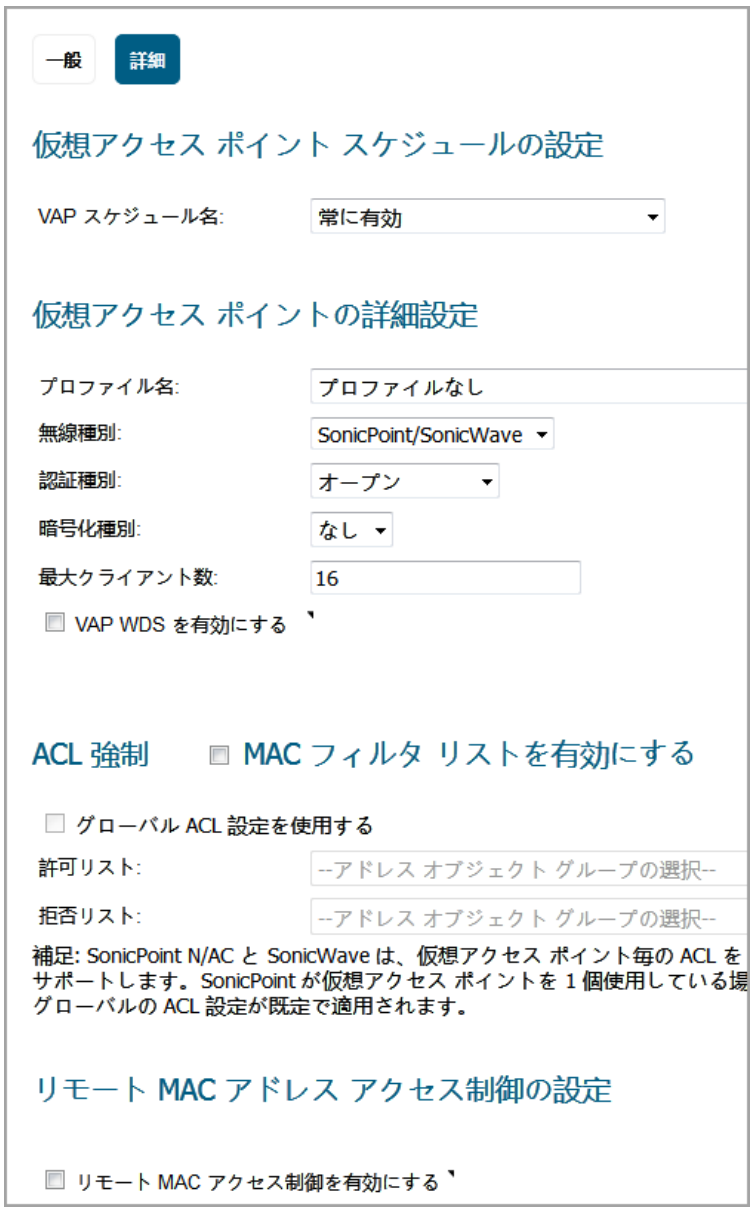
仮想アクセス ポイントの一般設定

機能	説明
名前	VAP のニックネームを作成します。
SSID	この VAP を使用するアクセス ポイントの SSID 名を入力します。この名前は、利用可能なアクセス ポイントを検索するときに、無線クライアントのリストに表示されます。
VLAN ID	VLAN をサポートしているプラットフォームを使用するときは、この VAP に関連付ける VLAN ID をオプションで選択できます。選択した VLAN から、この VAP のための設定が引き継がれます。
仮想アクセス ポイントを有効にする	この VAP を有効にします。このオプションは、既定では選択されています。

仮想アクセス ポイントの一般設定

機能	説明
SSID 抑制を有効にする	SSID 名のブロードキャストを抑止し、プローブ要求への応答を無効にします。このオプションをオンにすると、不正な無線クライアントから無線 SSID を確認できなくなります。このオプションは、既定では選択されていません。
動的 VLAN ID 割り当てを有効にする	有効にする場合、チェックボックスをオンにします。動的 VLAN は認証種別が EAP の場合にのみ設定できます。

詳細タブ



詳細設定では、特定の仮想アクセス ポイントに対して、認証と暗号化が設定できます。ユーザが作成したプロファイルからこれらの設定を引き継ぐには、**プロファイル名**を選択します。「**仮想アクセス ポイントを追加または編集する**」ウィンドウの「**詳細**」タブは、「**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**」ウィンドウと同じなので、認証と暗号化の設定の詳細については、「仮想アクセス ポイント プロファイル」を参照してください。

仮想アクセス ポイント グループ

仮想アクセス ポイント グループ機能は、SonicWall NSA 装置で利用できます。この機能ではアクセス ポイントに同時に適用する複数の VAP オブジェクトをグループ化することができます。仮想アクセス ポイント グループの設定は「**接続 | アクセス ポイント > 仮想アクセス ポイント**」ページで行います。

仮想アクセス ポイント グループを追加するには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して**編集**アイコンをクリックします。

4 「**仮想 AP グループ名**」フィールドに入力します。

5 オブジェクトをグループに追加するには、「**使用可能な仮想 AP オブジェクト**」リストから追加したいオブジェクトを選択して、「**右矢印**」をクリックし、「**仮想 AP グループのメンバー**」に移動させてください。

または、すべてのオブジェクトを追加するには、「**すべて追加**」を選択します。

6 オブジェクトをグループから削除するには、「**左矢印**」か、「**すべて削除**」ボタンを使用してください。

7 「**OK**」を選択して設定を保存します。

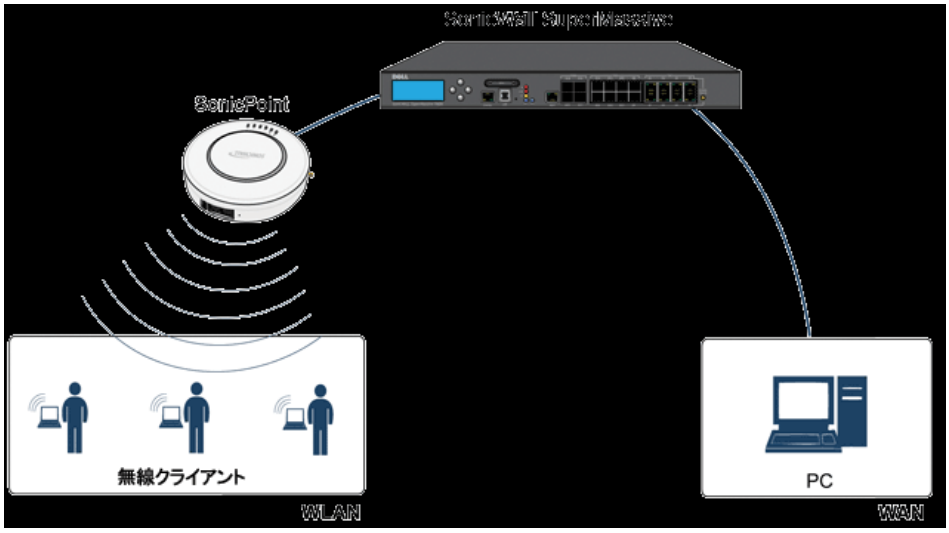
24

FairNet の設定

FairNet は、関連する無線クライアントの帯域幅を制御してクライアント間で帯域幅が公平に振り分けられるようにする、ネットワーク管理者向けの簡単に使えるツールです。管理者は、すべての無線クライアント、特定の IP アドレス範囲、または個々のクライアントに対して FairNet の帯域幅制限を設定することで公平性とネットワーク効率を向上させることができます。

以下に、典型的な FairNet トポロジの例を示します。

典型的な FairNet トポロジ



ノートパソコンまたは PC に IEEE802.11b/g/n 無線ネットワーク インターフェース コントローラを装備する必要があります。

トピック:

- サポート対象プラットフォーム
- FairNet の機能
- 管理インターフェースの概要
- FairNet の設定

サポート対象プラットフォーム

FairNet 機能は現在、次の装置モデルでサポートされています。

- SonicWall TZ シリーズ
- SonicWall NSA シリーズ

- SonicWall E-Class NSA シリーズ
- SonicWall SuperMassive シリーズ

FairNet の機能

Distributed Coordination Function (DCF) は、個々のクライアントが媒体にアクセスするとき等しい機会が得られるようタイミングの公平性を実現します。ただし、すべての無線クライアントの間でのステーション単位のデータ トラフィックの公平性を保証することはできません。FairNet 機能は既存の 802.11 DCF 上に実装され、フローの数や方向とは関係なく、無線クライアントの間での公平な帯域幅を保証します。

トラフィック制御機能は、(キューの長さが限界に達した場合やトラフィックが速度制限を超えた場合に) パケットをキューに入れるか破棄するかを判断しますパケットをどの順序で送信するか判断する (特定のパケットを優先する場合など)、パケットの送信を遅らせる (発信トラフィックの速度を制限する場合など) といったことも行います。トラフィック制御で送信対象として解放されたパケットは、デバイス ドライバに補足され、ネットワークに放出されます。

管理インターフェースの概要

FairNet 表示の要素を、以下のテーブルで説明します。

FairNet インターフェースの構成要素

名前	説明
ボタンとチェックボックス	
追加	特定の IP アドレスまたはアドレス範囲について FairNet ポリシーを追加します。「**Fairnet ポリシーの追加**」ダイアログが表示されます。
削除	選択した FairNet ポリシーを削除します。
適用	直前の構成の設定を適用します。
キャンセル	構成の設定の変更を取り消します。
チェックボックス	
FairNet を有効にする	FairNet 機能を有効にします。
FairNet ポリシー	「**FairNet ポリシー**」テーブルの見出しで、「**FairNet ポリシー**」テーブルのすべてのポリシーを選択または選択解除します。ポリシーのリストでポリシーを個別に選択することもできます。

FairNet インターフェースの構成要素

名前	説明
FairNet ポリシーテーブルの列	
方向	各ポリシーの方向を表示します。方向は、次のように区分されます。 • アップリンク • ダウンリンク • 両方
開始 IP アドレス	IP アドレス範囲の始点を表示します。
終了 IP アドレス	IP アドレス範囲の終点を表示します。
最低速度 (kbps)	クライアントに保証される最低帯域幅です。最低速度は 1Kbps です。
最大速度 (kbps)	クライアントに保証される最大帯域幅です。最大速度は 54000Kbps です。
インターフェース	FairNet ポリシーの適用先のインターフェースを表示します。これはアクセス ポイントが接続する管理ファイアウォールのインターフェースです。
有効	このチェックボックスをオンにすると、選択された FairNet ポリシーが有効になります。
設定	**編集**アイコンが選択された場合に、既存の FairNet ポリシーを編集します。特定の FairNet ポリシーを削除するには、**削除**アイコンをクリックします。

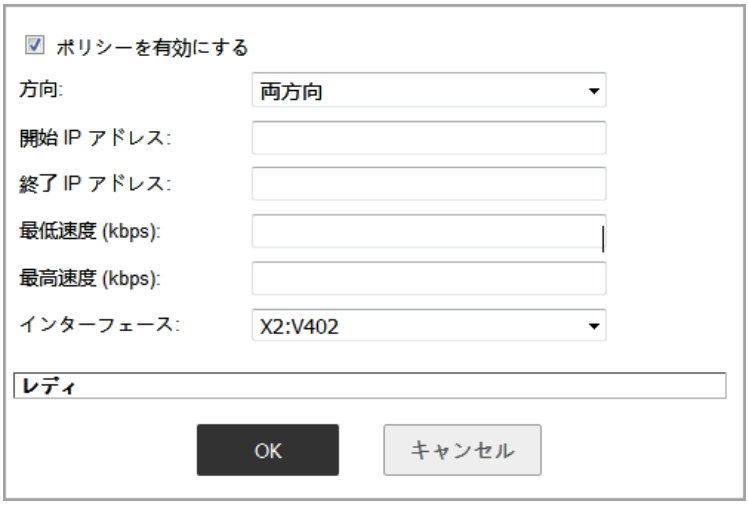
FairNet の設定

このセクションでは、FairNet の設定例を示します。

FairNet で両方向の帯域幅を広く設定するには、以下の手順に従います。

1 「**接続 | アクセス ポイント > FairNet**」ページに移動します。

2 「**追加**」ボタンを選択します。



3 「**ポリシーを有効にする**」チェックボックスをオンにします。これは既定でオンになっています。

4 「**方向**」ドロップダウン メニューから、「**両方向**」を選択します。これでポリシーはコンテンツのアップロードとダウンロードを行うクライアントに適用されます。このオプションは既定の設定です。

5 「**開始 IP アドレス**」フィールドを選択し、FairNet ポリシーの開始 IP アドレス (例えば、172.16.29.100) を入力します。

6 「**終了 IP アドレス**」フィールドを選択し、FairNet ポリシーの終了 IP アドレス (例えば、172.16.29.110) を入力します。

ヒント：この IP アドレス範囲は、WLAN インターフェースに関して設定されたサブネット上になければなりません。

7 「**最低速度 (kbps)**」フィールドに、FairNet ポリシーの最小帯域幅 を入力します。最小値かつ既定値は 100Kbps、最大値は 300Mbps (300,000Kbps) です。

8 「**最大速度 (kbps)**」フィールドに、FairNet ポリシーの最大帯域幅を入力します。最小値かつ既定値は 100Kbps、最大値は 300Mbps (300,000Kbps) です。ただし、通常の設定は 20Mbps です。

9 「**インターフェース**」ドロップダウン メニューから、アクセス ポイントの接続先のインターフェース (例えば、「X2」) を選択します。

10 「**OK**」ボタンをクリックすると、FairNet ポリシーが「**FairNet ポリシー**」テーブルに追加されます。

11 「**FairNet を有効にする**」チェックボックスをオンにします。

12 「**適用**」ボタンを選択します。

SonicWall FairNet ポリシーが設定されました。

25

Wi-Fi マルチメディアの設定

SonicOS アクセス ポイントは、Wi-Fi マルチメディア (WMM) をサポートし、無線 IEEE 802.11 ネットワーク上で帯域幅を大量に使用する VoIP、Wi-Fi 電話機上の VoIP、マルチメディア トラフィックなどのアプリケーションのサービス品質 (QoS) エクスペリエンスを高めます。

WMM は IEEE 802.11e 標準に基づく Wi-Fi Alliance の相互通信認証です。WMM では、以下の 4 つのアクセス種別に基づいてトラフィックに優先順位を付けます。

- **音声型** - 最も優先順位が高い
- **映像型** - 2 番目に優先順位が高い
- **最大努力型** - 3 番目に優先順位が高い (電子メールやインターネット サーフィンなどのアプリケーションを想定)
- **バックグラウンド型** - 4 番目に優先順位が高い (印刷など、遅延の影響を受けにくいアプリケーションを想定)

メモ：WMM は保証されたスループットを提供しません。

トピック:

WMM アクセス種別

それぞれのアクセス種別には自身の伝送キューがあります。トラフィックには、アプリケーションまたはファイアウォールのいずれかから提供されるサービス種別 (ToS) 情報に基づいて適切なアクセス種別が割り当てられます。SonicWall セキュリティ装置は、アクセス ルールまたは VLAN タギングのいずれかを介して ToS を割り当てます。

以下の表に、WMM アクセス種別と 802.1D ユーザ優先順位の対応関係を示します。

Wi-Fi マルチメディアのアクセス種別

優先順位	ユーザ優先順位 (802.1D ユーザ優先順位と同じ)	802.1D の指定	WMM アクセス種別 (AC)	WMM AC 指定 (情報)
最低	1	BK	AC_BK	バックグラウンド型
	2	-	AC_BK	バックグラウンド型
	0	BE	AC_BE	最大努力型
	3	EE	AC_BE	最大努力型
	4	CL	AC_VI	映像型
	5	VI	AC_VI	映像型
	6	VO	AC_VO	音声型
最高	7	NC	AC_VO	音声型

WMM は、拡張型分散チャンネル アクセス (EDCA) と呼ばれるプロセスによってトラフィックに優先順位を付けます。WMM は、アクセス種別ごとに異なる "バックオフ" 時間を定義してトラフィックに優先順位を付けます。WMM バックオフ時間は、以下の 2 つのパラメータで定義されます。

- **Arbitration Inter-Frame Space (AIFS)** - 無線チャンネルが無動作状態になってから、AC がチャンネルへのアクセスのネゴシエーションを開始できるようになるまでの時間間隔。
- **Contention Window (CW)** - ランダムなバックオフ時間のとり得る値の範囲。ランダムなバックオフ時間を指定する時間の範囲。CW は最小値と最大値で定義されます。
  - **Minimum contention window size (CWMin)** - CW の長さの最初の上限。AC は 0 ～ CWMin までのランダム時間待機してから伝送を試みます。優先順位の高い AC にはそれだけ短い CWMin が割り当てられます。
  - **Maximum contention window size (CWMax)** - CW の上限。競合が発生した場合、AC は CW のサイズを 2 倍にして (最大 CWMax まで) 伝送を再度試みます。CWMax は CWMin よりも大きい必要があります。

一般に、優先順位の高い AC には、AIFS、CWMin、CWMax の値が小さく設定されます。

メモ：AIFS、CWMin、および CWMax の測定単位は、使用されている 802.11 規格のスロット時間の倍数です。802.11b の場合、1 スロットは 20 マイクロ秒です。802.11a と 802.11g の場合、1 スロットは 9 マイクロ秒です。

アクセス ポイントとステーション (SonicWall セキュリティ装置) にそれぞれ異なる WMM パラメータが設定されます。以下のテーブルに、アクセス ポイントと SonicWall セキュリティ装置の既定の WMM パラメータを示します。

アクセス ポイントの既定の WMM パラメータ

WMM アクセス種別 (AC)	WMM AC 指定 (情報)	CWMin	CWMax	AIFS
AC_BE(0)	最大努力型	4	6	3
AC_BK(1)	バックグラウンド型	4	10	7
AC_VI(2)	映像型	3	4	1
AC_VO(3)	音声型	2	3	1

SonicWall セキュリティ装置の既定の WMM パラメータ

WMM アクセス種別 (AC)	WMM AC 指定 (情報)	CWMin	CWMax	AIFS
AC_BE(0)	最大努力型	4	10	3
AC_BK(1)	バックグラウンド型	4	10	7
AC_VI(2)	映像型	3	4	2
AC_VO(3)	音声型	2	3	2

アクセス種別へのトラフィックの割り当て

WMM はアクセス ポイントに対して、複数の優先順位アクセス種別に対して複数のキューを実装するように要求しています。アクセス ポイントは、アプリケーションまたはファイアウォールが提供する IP データ内のサービス種別 (TOS) 情報に基づいて、トラフィック種別を区別します。SonicWall セキュリティ装置は、WMM アクセス種別に以下の 2 つの方法でトラフィックを割り当てます。

- ファイアウォール サービスとアクセス ルールの指定
- VLAN タグ付け

ファイアウォール サービスとアクセス ルールの指定

特定のポートを使用するサービスに優先順位を付けて、適切な伝送キューに入れます。例えば、ポート 2427 に送信される UDP トラフィックをビデオ ストリームとみなすことができます。「**ポリシー | オブジェクト > サービス オブジェクト**」ページにユーザ定義サービスを追加します。詳細については、*SonicOS 6.5 ポリシー*を参照してください。

新しいサービスに対して少なくとも 1 つのアクセス ルールが「**ポリシー | ルール > アクセス ルール**」ページで追加されている必要があります。例えば、そのようなサービスが LAN ゾーン上のステーションから WLAN ゾーン上の無線クライアントに対して行われる場合は、アクセス ルールを「**ルールの追加**」ウィンドウの「**一般**」タブで設定できます。「**ルールの追加**」ウィンドウの「**QoS**」タブでは、明示的な DSCP 値が定義されます。

後に、送信先ポート 2427 で UDP プロトコルを使用してパケットがファイアウォールを通してアクセス ポイントに送信されるときに、それらの TOS フィールドはアクセス ルール内の QoS 設定に従って設定されます。

VLAN タグ付け

SonicWave、SonicPoint N および AC では、同一の VLAN ID を使用して VLAN と接続するように仮想アクセス ポイントを設定できるため、仮想アクセス ポイントを介した VLAN 内の優先順位付けが可能です。VLAN トラフィックに対する優先順位はファイアウォール アクセス ルールを通して設定可能です。

ファイアウォール アクセス ルールは、例えば 2427 番ポートに向けられた UDP サービスに対する優先順位を設定するのと同様ですが、**送信元** と **送信先** は WLAN から WLAN へのルールであるため、WLAN サブネットのような VLAN (VAP を介した VLAN) インターフェースで設定します。ポリシー | ルール > アクセス ルール *SonicOS 6.5 ポリシー*に移動します。

Wi-Fi マルチメディア パラメータの設定

既定では、単一の WMM プロファイルが SonicWall セキュリティ装置に設定され、パラメータは 802.11e 規格の値に設定されます。

トピック:

- WMM の設定
- アクセス ポイントの WMM プロファイルの作成
- WMM プロファイルの削除

WMM の設定

WMM 設定をカスタマイズするには、以下の手順に従います。

1 「**接続 | アクセス ポイント>Wi-Fi マルチメディア**」ページに移動します。

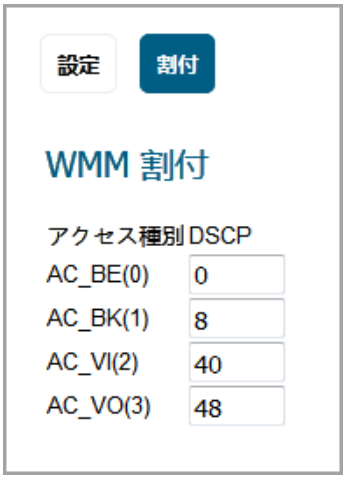
2 WMM プロファイルを変更するには、そのプロファイルに対する**編集**アイコンを選択します。あるいは、新しい WMM プロファイルを作成する場合は、「**追加**」ボタンを選択します。

3 新しい WMM プロファイルを作成する場合は、「**プロファイル名**」を入力します。既定の名前は、**wmmDefault** です。

4 パラメータを変更して WMM プロファイルをカスタマイズします。既定値の WMM パラメータ値が、自動的に精製されたウィンドウに表示されます。これらの種別については、「Wi-Fi マルチメディアのアクセス種別」テーブルを参照してください。

メモ：WMM プロファイルを設定するときに、コンテンション ウィンドウのサイズ (CWMin/CWMax) と、AIFS (フレーム送信間隔) を設定できます。これらの値は、アクセス ポイント (SonicPoint-N) とステーション (ファイアウォール) 上の AC_BK、AC_BE、AC_VI、AC_VO の各優先順位に対して、個別に設定可能です。

5 「**割付**」タブを選択して、アクセス種別と DSCP 値の割付をカスタマイズします。



6 割付優先順位レベルを DSCP 値に対応付けることができます。既定の DSCP 値は **ポリシー | ルール > アクセス ルール の QoS** 割付内のものと同じです。

7 「**OK**」を選択します。

アクセス ポイントの WMM プロファイルの作成

「**管理**」表示の「**接続 | アクセス ポイント > Wi-Fi マルチメディア**」ページは、WMM プロファイルの設定および優先順位割付の設定方法を提供します。

「**アクセス ポイント > 基本設定**」ページから SonicWave、SonicPoint N、SonicPoint AC を設定する際、既存の WMM プロファイルを選択して WMM プロファイルを作成できます。「**設定**」ウィンドウでは、「**無線 0 詳細**」、「**無線 1 詳細**」の各タブに「**WMM (Wi-Fi マルチメディア)**」ドロップダウン メニューがあります。

「**WMM (Wi-Fi マルチメディア)**」ドロップダウン メニューから「**WMM プロファイルの作成...**」を選択すると、「**WLAN WMM プロファイルの追加**」ウィンドウが表示されます。

WMM プロファイルの削除

1 つの WMM プロファイルを削除するには、そのプロファイルの「**設定**」列の**削除**アイコンを選択します。

複数の WMM プロファイルを削除するには、削除するプロファイルのチェックボックスをオンにしてから「**削除**」ボタンを選択します。

すべての WMM プロファイルを削除するには、「**すべて削除**」ボタンを選択します。すべてのプロファイルが削除されることを確認するポップアップ メッセージが表示されます。

26

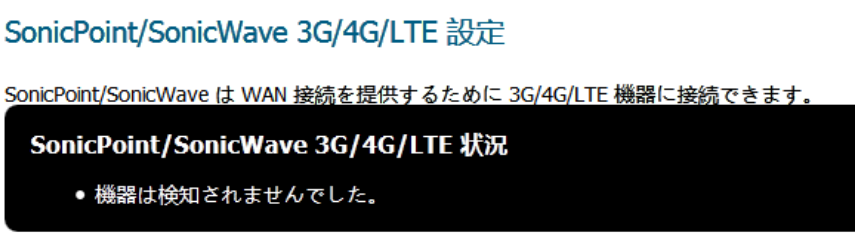
アクセス ポイント 3G/4G/LTE WWAN

アクセス ポイントに接続された 3G/4G/LTE 機器があれば、「**接続 | アクセス ポイント > 3G/4G/LTE WWAN**」ページでその機器に対する監視情報が提供されます。

最初のパネルは接続データとモデム状況を提供し、2 番目のパネルには機器の信号強度をグラフィック表示します。

パネルのデータを更新するには、再表示ボタンを選択します。

3G/4G/LTE 機器がアクセス ポイントに検出できない場合、「**接続 | アクセス ポイント > 3G/4G/LTE WWAN**」ページに以下のメッセージが表示されます。



27

Bluetooth LE デバイスの表示

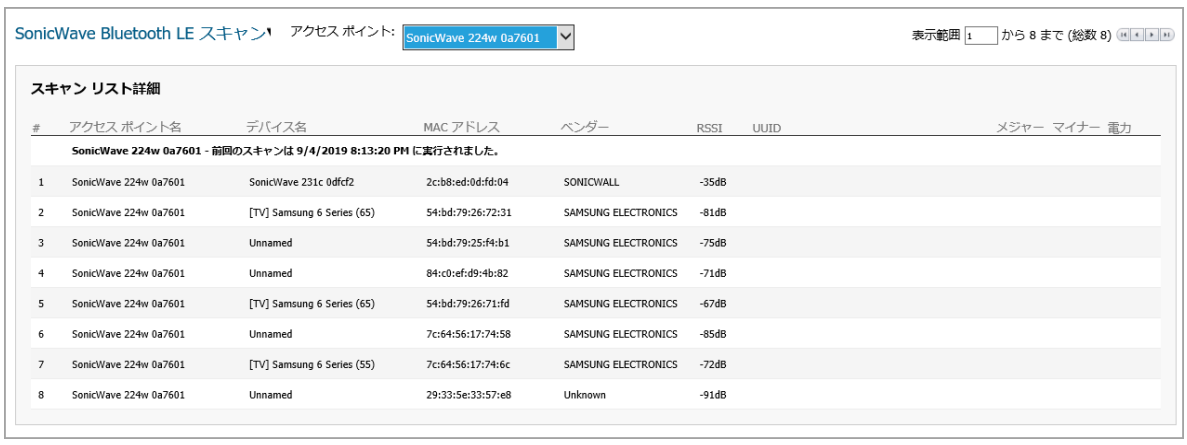
SonicWave 432 および 200 シリーズの装置は、Bluetooth 低消費電力 (BLE) をサポートするようになりました。Bluetooth 低消費電力とは、標準の Bluetooth 装置と同程度の通信範囲を維持しつつ、消費電力とコストを大幅に削減する、無線パーソナル エリア ネットワーク技術です。Bluetooth 低消費電力 (BLE) は、特に iBeacon 装置に近接している場合に、スマートフォン、タブレット、SonicWall モバイル アプリ、および他の SonicWave などの他のデバイスが SonicWave アクセス ポイントに簡単に接続できるようにする標準的な Bluetooth のサブセットです。BLE は、位置推定と、より簡単な SonicWave 設定も提供します。

メモ：iBeacon はアップルが開発したプロトコルです。さまざまなベンダーが、近くの携帯電子機器に識別子をブロードキャストする iBeacon 互換の BLE 機器を製造しています。このテクノロジにより、スマートフォン、タブレット、その他のデバイスは、iBeacon の近くにいるときにアクションを実行できます。

BLE スキャン データの表示

「**管理 | 接続性 > アクセス ポイント > Bluetooth LE**」ページには、近くの Bluetooth 低消費電力 (BLE) デバイスに関する情報が表示されます。ページ上部の「**アクセス ポイント**」ドロップダウン リストから単一の SonicWave または**すべてのアクセス ポイント**を選択することにより、表示を制御できます。

SonicWave で iBeacon を有効にする方法については、「プロビジョニング プロファイルの Bluetooth LE 設定 (214 ページ)」を参照してください。

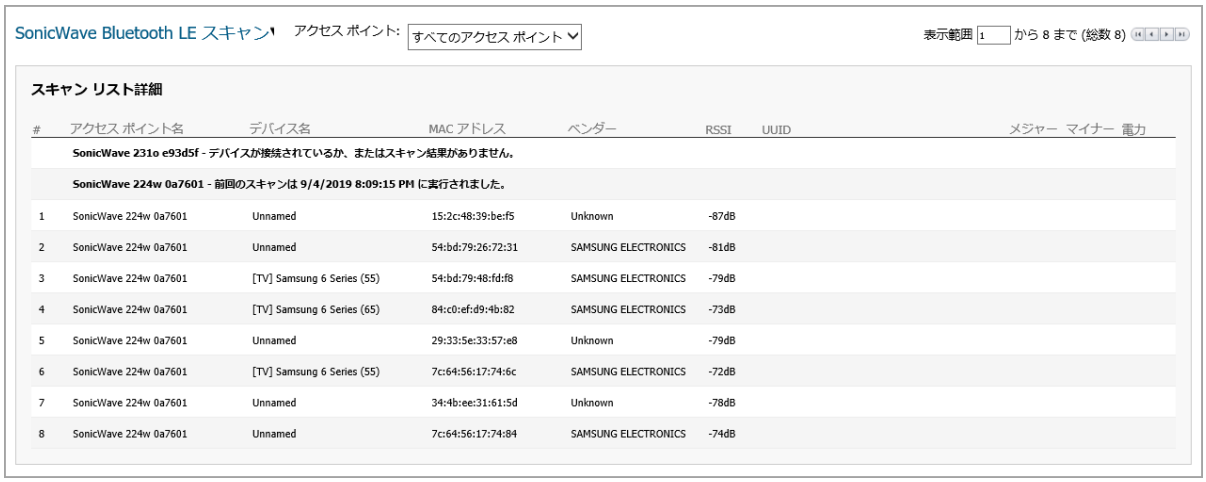


「**スキャン リストの詳細**」テーブルには、近くの BLE デバイスからスキャンされた情報が表示されます。使用可能な場合、列には次の情報が表示されます。

列	説明
#	テーブル行の参照番号。
アクセス ポイント名	BLE デバイスをスキャンするアクセス ポイント (SonicWave) の名前。

列	説明
デバイス名	BLE デバイスの名前。
MAC アドレス	デバイスの一意のハードウェア アドレス。
ベンダー	デバイスの製造元。
Rssi	負の数 (dB) で表される、BLE デバイスの受信信号強度インジケータ。数値が大きい (ゼロに近い) ほど、信号は強くなります。
UUID	BLE デバイスの一意の識別子である近接 UUID。ちょうど 36 個の、16 進文字とハイフン。 すべてゼロには設定しないでください。
メジャー	BLE デバイス グループ内の上位の ID。有効な値は 0-65535 です。 0x0000 = 設定解除。
マイナー	BLE デバイス グループ内の下位の ID。有効な値は 0-65535 です。 0x0000 = 設定解除。
電源	BLE デバイスの電力レベル (dBm)。これは、スキャンされたデバイスの***測定電力***です。Apple で定義されたある方法と同等の方法で複数の RSSI サンプルを平均化することにより計算されます。

次の画像は、このデータの一部を示しています。



第 4 部

接続性 | 無線

- 無線の概要
- 無線の設定
- 無線セキュリティの設定
- 無線の詳細設定
- 無線 > MAC フィルタ リスト
- 無線 IDS の設定
- 内部ワイヤレス無線機を備えた仮想アクセス ポイントの設定

28

無線の概要

「**管理 | 接続性 | 無線**」の下にあるページで装置の無線設定を行うことができるのは、SonicWall 無線セキュリティ装置だけです。

メモ：SonicOS 6.5.3 以降では、「**管理 | システム セットアップ | 装置 > 基本設定**」ページで「**無線制御モード**」が「**フル機能ゲートウェイ**」か「**無線制御のみ**」に設定されているとき「**無線**」ページが表示されます。「**無線なし**」が「**無線制御モード**」で有効になっている場合、「**無線**」メニューの見出しとその下のページは表示***されません***。詳細については、『*SonicOS 6.5 システム設定* 管理ガイド』を参照してください。

SonicWall 無線セキュリティ装置は、IEEE802.11a、IEEE 802.11ac、IEEE 802.11b、802.11g、および 802.11n という無線プロトコルをサポートしており、無線伝送でデータを送信します。これらの無線伝送は一般に Wi-Fi として知られています。SonicWall 無線セキュリティ装置は、アクセス ポイント、セキュア無線ゲートウェイ、および、NAT や VPN の柔軟な開始と停止が可能なステートフル ファイアウォールという 3 つのネットワーク コンポーネントを組み合わせて、全面的に安全な無線ファイアウォールを提供します。この組み合わせにより、無線セキュリティ装置は、ネットワーク セキュリティを損なうことなく無線の柔軟性を実現します。

通常、無線セキュリティ装置は、無線 LAN のアクセス ポイントになり、LAN 上のコンピュータのセントラル アクセス ポイントの役割を果たします。また、1 つのブロードバンド接続をネットワーク上のコンピュータと共有します。無線セキュリティ装置はファイアウォール保護も提供するので、インターネットからの侵入者はネットワーク上のコンピュータやファイルにアクセスできません。これは、ネットワーク上のコンピュータ間で共有している DSL 回線や T1 回線などの "常時稼働" 接続にとって特に重要です。

ただし、無線 LAN は他の無線ネットワークから "傍受" されやすいので、無線 LAN には無線セキュリティ ポリシーを確立する必要があります。無線セキュリティ装置では、無線クライアントはファイアウォールのアクセス ポイント レイヤに接続します。有線ネットワークに接続を直接ブリッジする代わりに、無線トラフィックはまず、保護された無線ゲートウェイ レイヤへ渡され、クライアントはそこでユーザ レベル認証で認証される必要があります。ゲスト サービスと MAC フィルタ リストへの無線アクセスは無線セキュリティ装置によって管理されます。すべてのセキュリティ条件を満たすと、無線ネットワーク トラフィックは以下のいずれかの配信システムを通過できます。

- LAN
- WAN
- WLAN 上の無線クライアント
- DMZ または Opt ポート上のその他のゾーン
- VPN トンネル

トピック:

- 機器サポート
- 遵守
- 無線接続を使用する場合の考慮事項

- アンテナの調整
- 無線ノード数の強制
- MAC フィルタ リスト

機器サポート

SonicOS がサポートする無線機器には、以下のようなものがあります。

- TZ500W
- TZ400W
- TZ350/350W
- TZ300W
- SOHO W
- SOHO 250/250W
- SonicWave 231c
- SonicWave 231o
- SonicWave2 AC 2x2c

遵守

無線機器を特定の国や地域で販売・使用するには、さまざまな必要条件を遵守する必要があります。SonicWall 無線機器に関する利用認可と制限の最新情報については、https://www.sonicwall.com/ja-jp/support で対象製品のドキュメントを参照してください。機器ごとに、固有の利用認可ドキュメント、または関連情報を提供する『*導入ガイド*』があります。

FCC U-NII の新しい規則への準拠

SonicOS 6.2.5.1 以降では、FCC U-NII (Unlicensed -National Information Infrastructure) の新しい規則 (Report and Order ET Docket No. 13-49) が TZ シリーズおよび SOHO 無線装置でサポートされます。動的周波数選択 (DFS) に関する FCC の新しい規則に準拠するために、TZ シリーズまたは SOHO 無線装置は DFS バンドのレーダー信号を検出してレーダー信号との干渉を回避します。

メモ：FCC の新しい規則に準拠したファームウェアを使用して製造された TZ シリーズおよび SOHO 無線装置は、SonicOS 6.2.5.1 以降でのみサポートされています。

RED 遵守

SonicOS 6.5 以降では、TZ シリーズおよび SOHO 無線装置は無線機器指令 (RED) をサポートしています。RED (2014/53/EU) は、安全性、衛生、電磁的適合性および電波スペクトルの効率的な使用に対する重要な必要事項を規定しています。

無線接続を使用する場合の考慮事項

無線接続を有線接続と比較して検討する際には、インフラおよび環境に対する利点と欠点を考慮してください。

モビリティ	ネットワークの大多数はノートパソコンですか？無線接続は有線接続より移動性に優れています。
利便性	無線ネットワークでは、各コンピュータをケーブルでつないだり、コンピュータ ケースを開けてネットワーク カードをインストールしたりする必要がありません。
速度	ネットワーク速度が重要な場合は、無線接続よりイーサネット接続を使用することを検討してください。
到達範囲	ネットワーク環境に物理的な障害物や干渉要素が多い場合、無線ネットワークは適さない可能性があります。
セキュリティ	無線伝送の持つ無制約な性質上、無線ネットワークには本質的なセキュリティ問題があります。ただし、無線セキュリティ装置はファイアウォールであり、その NAT 機能でセキュリティを提供しており、WPA または WPA2 を使用してデータ伝送を保護できます。

最適な無線パフォーマンスのための推奨事項

最適な無線パフォーマンスのために、SonicWall は以下を推奨します。

- 無線セキュリティ装置は、目的のネットワークの中心近辺に配置します。こうすることによって、近隣の無線ネットワークから傍受される可能性も低減できます。
- 無線セキュリティ装置と PC やノートパソコンなどの受信ポイントの間の壁や天井の数を最小限にします。
- 無線セキュリティ装置は、できる限り、他の無線コンポーネントから直線で結ばれる位置に配置するようにします。無線コンポーネント同士が直接見える位置にあると、最高のパフォーマンスが得られます。
- 建築構造によっても無線パフォーマンスに違いが出ることがあります。
    - 無線セキュリティ装置は、壁や暖炉など大きくて隙間のない物体の近くに置かないようにします。
    - 無線セキュリティ装置をコンピュータ ケース、モニタ、装置など金属製の物の近くに置くと、そのユニットのパフォーマンスが低下することがあります。
    - 金属製フレーム、窓ガラス用 UV カット フィルム、コンクリート造または石造の壁、金属塗料などの近くに無線セキュリティ装置を設置した場合も、信号強度が低下することがあります。
- 建物の上階では、無線セキュリティ装置を高い場所に設置すると、障害物を回避してパフォーマンスを向上させることに役立ちます。
- 近隣の無線ネットワークや無線機器によって、無線セキュリティ装置の信号強度、速度、到達範囲が影響を受けることがあります。
- コードレス電話、ラジオ、電子レンジ、テレビなどの機器によって、無線セキュリティ装置に干渉が発生する可能性もあります。

アンテナの調整

無線セキュリティ装置のアンテナを調整して、無線受信状態が最もよくなるようにします。まず、アンテナをまっすぐ上に立て、それから必要に応じて調整します。無線セキュリティ装置の真下など、一部、相対的に受信状態の悪い領域があります。アンテナを別の無線機器に直接向けても、受信状態の向上にはつながりません。干渉が発生する可能性があるので、アンテナを金属製のドアや壁の近くに配置しないでください。

無線ノード数の強制

WLAN に接続しているか、SonicWall GroupVPN 経由で接続しているユーザは、SonicWall のノード数強制に加算されません。LAN および Opt ポート上の無線ゾーン以外のユーザのみ、ノード数制限に加算されます。

「ステーション状況」テーブルには、接続されているすべての無線ノードが表示されます。

MAC フィルタ リスト

SonicWall 無線セキュリティ装置のネットワーク プロトコルは、ネイティブの MAC アドレス フィルタリング機能を提供します。MAC アドレス フィルタリングを有効にすると、802.11 レイヤでフィルタリングが行われ、無線クライアントは認証と無線アクセス ポイントへの参加ができなくなります。認証と参加なしにはデータ通信は行えないので、クライアントが無線ネットワーク カードの Mac アドレスをネットワーク管理者に提示するまではネットワークへのアクセスは許可されません。

29

無線の設定

無線装置は、アクセス ポイント、無線クライアント ブリッジ、またはアクセス ポイントとステーションとしてセットアップできます。

802.11 無線アンテナの設定を行うには、以下に従います。

1 「**管理**」表示の「**接続 | 無線 > 基本設定**」ページに移動します。

2 装置に実行させたい「**無線の役割**」を選択します。

重要：モードを変更すると、クライアントが切断され、再起動が必要になります。

メモ：どの「**無線の役割**」を選択したかに応じて、ページ内のオプションの表示は変わります。

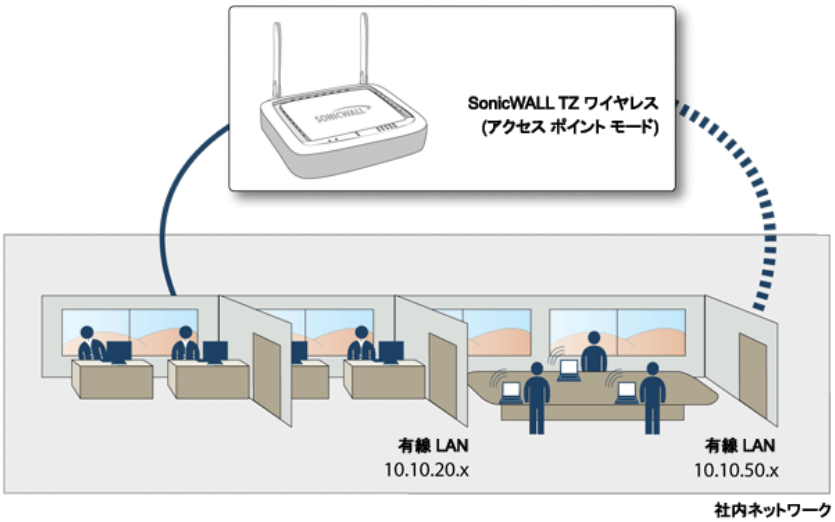
以下のセクションでは、個々の「**無線の役割**」オプションに対する設定方法について説明します。

- アクセス ポイント
- 無線クライアント ブリッジ
- アクセス ポイントとステーション

アクセス ポイント

「**無線の役割**」として「**アクセス ポイント**」を選択した場合、SonicWall を下図に示すような無線クライアントに対するインターネット/ネットワーク ゲートウェイとして設定することになります。

無線のモード: アクセス ポイント



トピック:

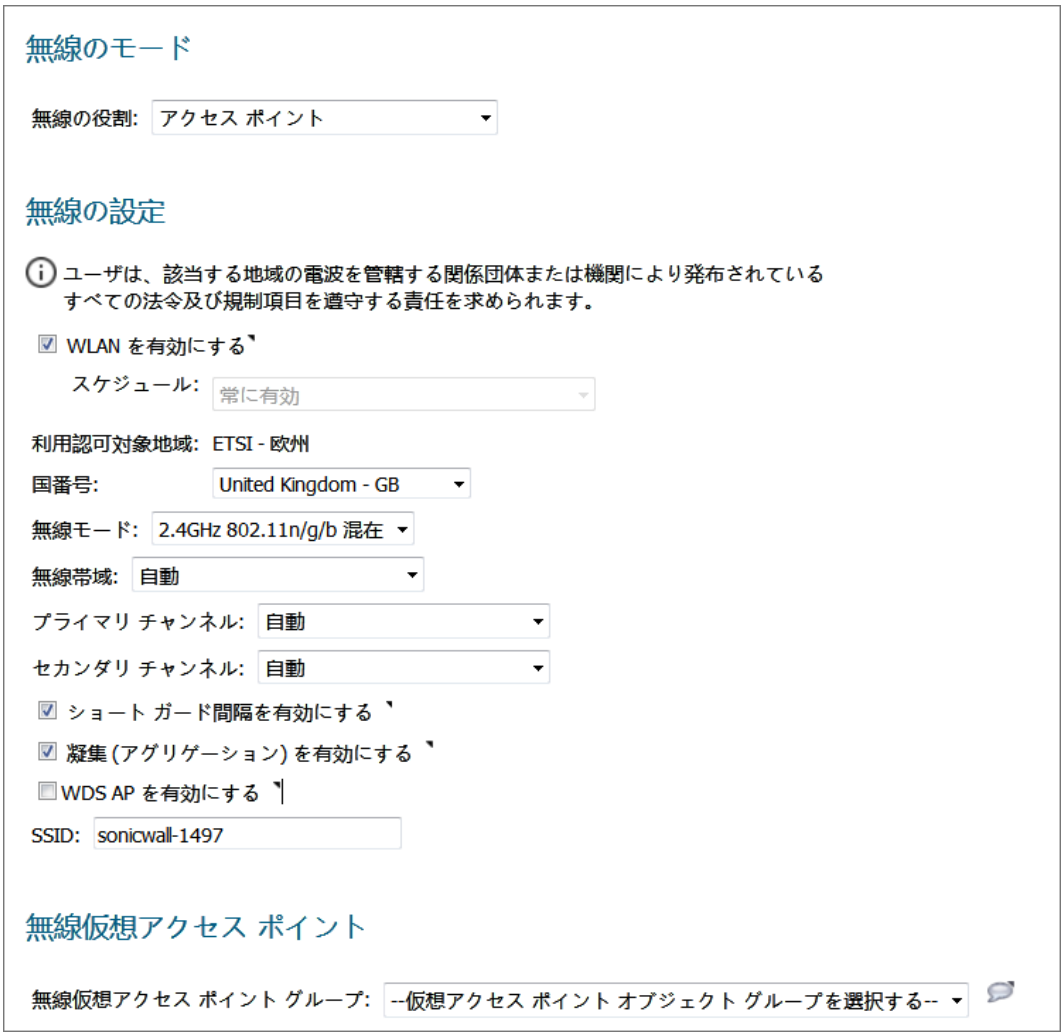
- アクセス ポイント無線の設定
- アクセス ポイント 無線仮想アクセス ポイント

アクセス ポイント無線の設定

重要：無線装置をアクセス ポイントとして設定する場合、無線運用者は、該当する地域の電波を管轄する関係団体または機関により発布されているすべての法令や規制を遵守する責任を負います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 基本設定**」を選択します。



3 「**無線の役割**」フィールドで、「**アクセス ポイント**」をドロップダウン メニューから選択します。

4 「**WLAN を有効にする**」チェックボックスをオンにします。これによって、モバイル ユーザにクリーンな無線アクセスを提供できます。「**適用**」を選択して設定を有効にします。WLAN 無線は既定では無効になっています。

5 「**スケジュール**」フィールドで、ドロップダウン メニューから WLAN 無線をアクティブにする時間を選択します。スケジュール リストには、「**システム セットアップ | 装置 > システム スケジュール**」ページで作成および管理するスケジュール オブジェクトが表示されます。既定値は「**常に有効**」です。

6 「**国番号**」フィールドには、アクセス ポイントが使用される国を選択してください。国番号は、どの利用認可対象地域の管轄で無線を利用するかを決定します。

7 「**無線モード**」フィールドには、ドロップダウン メニューから適切な無線モードを選択します。無線セキュリティ装置では、次のモードがサポートされています。

> **ヒント**：802.11n クライアントだけを対象に最適なスループット速度を実現するには、「**802.11n のみ**」無線機モードをお勧めします。複数の無線クライアント認証の互換性を維持するには、「**802.11n/g/b 混在**」無線モードを使用してください。

- **802.11n/a/ac 混在** - 802.11a、802.11ac、および 802.11n のクライアントが無線ネットワークにアクセスする場合は、このモードを選択します。
- 「**802.11ac のみ**」- 802.11ac クライアントだけが無線ネットワークにアクセスする場合は、このモードを選択します。

無線モード	定義
2.4GHz 802.11n/g/b 混在	802.11b、802.11g、および 802.11n のクライアントを同時にサポートします。無線ネットワークが複数の種類のクライアントで構成されている場合は、このモードを選択してください。
2.4GHz 802.11n のみ	802.11n クライアントだけが無線ネットワークにアクセスできます。この制限付き無線機モードでは、802.11a/b/g クライアントは接続できません。
2.4GHz 802.11g/b 混在	802.11g と 802.11b クライアントを同時にサポートします。無線ネットワークが両方の種別のクライアントで構成されている場合は、このモードを選択してください。
2.4GHz 802.11g のみ	無線ネットワークが 802.11g クライアントだけで構成されている場合は、802.11g パフォーマンスを向上させるためにこのモードを選択できます。このモードを選択すると、802.11b クライアントの参加を防ぐことができます。
5GHz 802.11n/a 混在	802.11a と 802.11n のクライアントが無線ネットワークにアクセスする場合は、このモードを選択します。
5GHz 802.11n のみ	802.11n クライアントだけが無線ネットワークにアクセスする場合は、このモードを選択します。
5GHz 802.11a のみ	802.11a クライアントだけが無線ネットワークにアクセスする場合は、このモードを選択します。
5GHz 802.11n/a/ac 混在	802.11a、802.11n、および 802.11ac のクライアントが無線ネットワークにアクセスする場合は、このモードを選択します。
5GHz 802.11ac のみ	スループットを向上させたい場合に選択してください。

無線設定セクションの残りのオプションは、選択した無線モードに応じて表示が変化する場合があります。

トピック:

- 802.11n の無線設定
- 802.11a/b/g の無線設定
- 802.11ac の無線設定

802.11n の無線設定

「**無線モード**」フィールドが 802.11n のみ、または 802.11n を含む混在モードに設定された場合、以下のオプションを設定します。

メモ：設定する装置の種別に応じて、実際に表示されるオプションは多少変わる場合があります。

無線帯域	802.11n の無線帯域を設定します
自動	装置は信号の強度と整合性に基づいて、無線動作に最適なチャンネルを自動的に検出および設定できます。このオプションは既定の設定です。
標準 - 20 MHz チャンネル	802.11n 無線が標準 20MHz チャンネルのみを使用するように指定します。このオプションを選択すると、「**標準チャンネル**」ドロップダウン メニューが表示されます。
標準チャンネル	既定値は**自動**であり、装置は信号の強度と整合性に基づいて最適なチャンネルを設定します。オプションで、利用認可対象地域内の単一のチャンネルを選択することもできます。特定のチャンネルを選択すると、エリア内の他の無線ネットワークとの干渉を防ぐのにも役立ちます。
広域 - 40 MHz チャンネル	802.11n 無線が広域 40MHz チャンネルのみを使用するように指定します。このオプションを選択すると、「**プライマリ チャンネル**」および「**セカンダリ チャンネル**」ドロップダウン メニューが表示されます。
プライマリ チャンネル	既定値は**自動**であり、特定のプライマリ チャンネルを指定することもできます。
セカンダリ チャンネル	このドロップダウン メニューの設定は、プライマリ チャンネルでの選択によって決まります。 • プライマリ チャンネルを「自動」に設定すると、セカンダリ チャンネルも「自動」に設定されます。 • プライマリ チャンネルを特定のチャンネルに設定すると、セカンダリ チャンネルはそのプライマリ チャンネルとの干渉を防ぐ最適なチャンネルに設定されます。
ショート ガード間隔を有効にする	サポートされている場合、これを有効にすると送信/受信速度が向上します。802.11ac/n モードにのみ適用されます。
凝集 (アグリゲーション) を有効にする	802.11n フレーム集約を有効にすることによって、複数のフレームを結合してオーバーヘッドを減らしスループットを向上させます。802.11ac/n モードにのみ適用されます。
WDS AP を有効にする	WDS クライアントがこのアクセス ポイントに接続できるようにします。
SSID	既定値は、**sonicwall-** に BSSID の最後の 4 文字を付加したもの (例: `sonicwall-C587`) になります。SSID は、32 文字以内の任意の英数字に変更できます。

ヒント：「**ショートガード間隔を有効にする**」オプションと「**凝集 (アグリゲーション) を有効にする**」オプションを選択すると、スループットを若干向上させることができます。どちらも、信号強度が高く干渉がほとんどない最適なネットワーク条件において、最も効果的です。最適とは言えない条件下 (干渉がある、信号強度が低いなど) のネットワークでは、これらのオプションが原因で伝送エラーが発生することがあるので、スループット向上効果は得られません。

802.11a/b/g の無線設定

「**無線モード**」フィールドが 802.11a のみ、802.11g/b 混在、または 802.11b のみに設定された場合、以下のオプションの設定が表示されます。

チャンネル	装置は信号の強度と整合性に基づいて、無線動作に最適なチャンネルを自動的に検出および設定できます。このオプションは既定の設定です。オプションで、利用認可対象地域内の単一のチャンネルを選択することもできます。
WDS AP を有効にする	WDS クライアントがこのアクセス ポイントに接続できるようにします。
SSID	既定値は、**sonicwall-** に BSSID の最後の 4 文字を付加したもの (例: `sonicwall-C587`) になります。SSID は、32 文字以内の任意の英数字に変更できます。

802.11ac の無線設定

802.11ac のみに無線機を設定すると、次のオプションが表示されます。

- 無線帯域ドロップダウン メニュー - 広域 - 80 MHz チャンネルのサポートを許容する、802.11ac 無線の帯域を設定します。
- 「**チャンネル**」ドロップダウン メニュー - チャンネルを選択します。
  - 「**自動**」- 無線セキュリティ装置は信号の強度と整合性に基づいて、無線動作に最適なチャンネルを自動的に検出および設定できます。「**自動**」は既定のチャンネル設定であり、この設定では、選択されている動作中のチャンネルが右側に表示されます。これ以外に、利用認可対象地域内のチャンネルを明示的に定義することもできます。
  - 特定のチャンネル - 利用可能なチャンネルについては、「プロビジョニング プロファイルの 5GHz/2.4GHz 無線の基本設定」を参照してください。

アクセス ポイント 無線仮想アクセス ポイント

無線仮想アクセス ポイントを使用する場合、「**仮想アクセス ポイント**」セクションのドロップダウン メニューから「**仮想アクセス ポイント グループ**」を選択してください。または、定義済の VAP グループを選択することもできます。

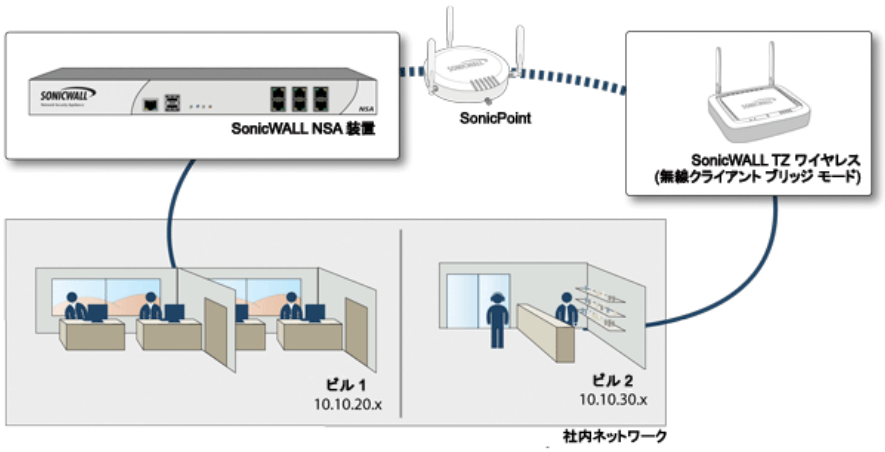
すべてのアクセス ポイント設定が終了したら、「**適用**」を選択して設定を保存します。

無線クライアント ブリッジ

無線装置は、別の SonicWall 無線装置または SonicPoint アクセス ポイントに無線でブリッジすることによって、インターネット/ネットワーク アクセスを提供します。「無線のモード: 無線クライアント ブリッジ 」を参照してください。「**無線クライアント ブリッジ**」モードを「**無線の役割**」として選択すると、物理的に離れている場所の間で、長くてコストのかかるイーサネット ケーブル接続を必要とすることなく、保護されたネットワーク通信ができるようになります。

メモ：無線仮想アクセス ポイントの使用中は、装置を無線クライアント ブリッジとして使用することはできません。

無線のモード: 無線クライアント ブリッジ



メモ：無線クライアント ブリッジの詳細については、http://www.SonicWall.com/us/support.html で提供されている『*SonicWall Secure Wireless Network Integrated Solutions Guide*』、または Technote 「*SonicWall Wireless Bridging*」を参照してください。

トピック:

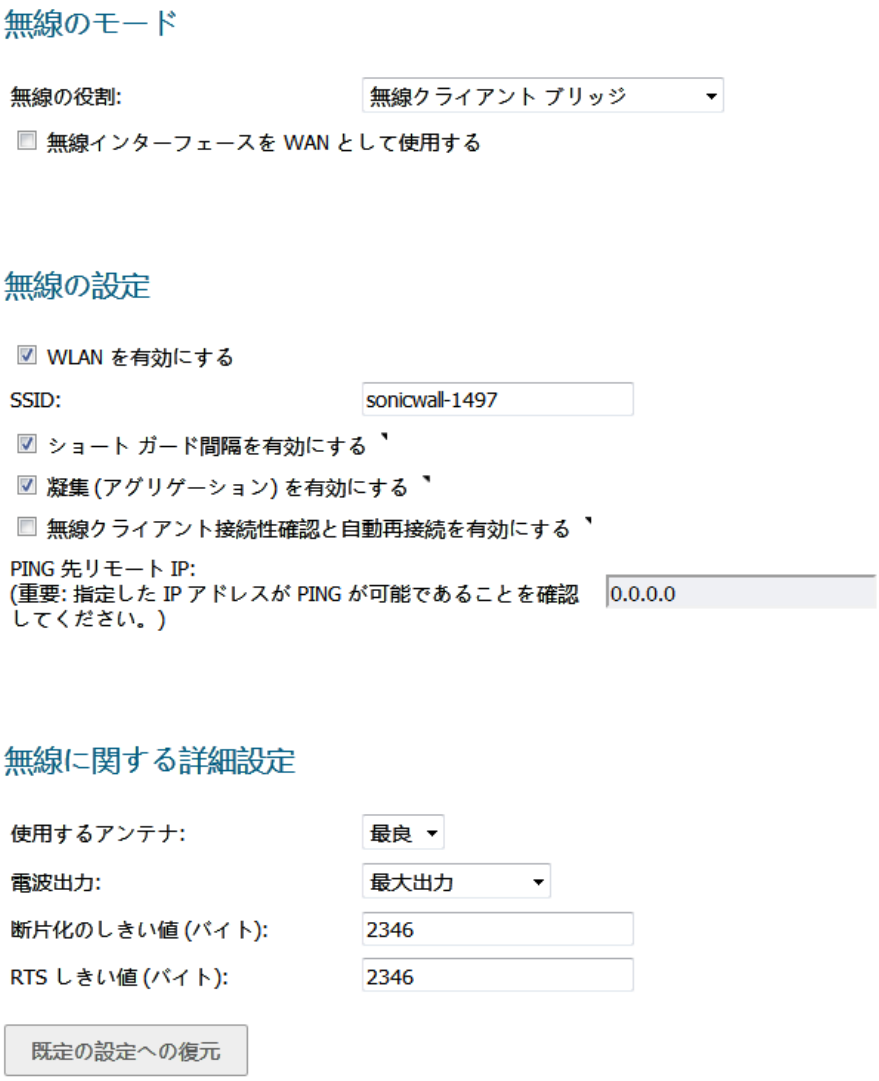
- クライアント ブリッジ無線の設定
- クライアント ブリッジ 無線詳細設定

クライアント ブリッジ無線の設定

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 基本設定**」を選択します。

3 「**無線の役割**」フィールドで、「**無線クライアント ブリッジ**」をドロップダウン メニューから選択します。



4 **無線インターフェースを WAN として使用する**場合にはチェックボックスをオンにします。既定値はオフです。

5 「**無線の設定**」セクションで、「**WLAN を有効にする**」チェックボックスをオンにします。クライアント ブリッジ モードでは、無線が有効になるとアクセス ポイントではなくクライアントとして動作し、クライアントに対する無線アクセスは提供しません。「**適用**」を選択して設定を有効にします。WLAN 無線は既定では無効になっています。

6 以下のオプションを選択します

SSID	既定値は、**sonicwall-** に BSSID の最後の 4 文字を付加したもの (例: `sonicwall-C587`) になります。SSID は、32 文字以内の任意の英数字に変更できます。
ショート ガード間隔を有効にする	サポートされている場合、これを有効にすると送信/受信速度が向上します。802.11ac/n モードにのみ適用されます。
凝集 (アグリゲーション) を有効にする	802.11n フレーム集約を有効にすることによって、複数のフレームを結合してオーバーヘッドを減らしスループットを向上させます。802.11ac/n モードにのみ適用されます。

無線クライアント接続性確認と自動再接続を有効にする	定期的に、ユーザが定義した IP アドレスに ping を行うことで無線クライアント接続性を確認します。接続が失われている場合、自動再接続を実行します。
PING 先リモート IP	上記の接続性確認を有効にした場合、ping を実行する先のリモート IP を入力します。 重要：指定した IP アドレスが ping を返すことを確認してください。

クライアント ブリッジ 無線詳細設定

無線に関する詳細設定を行うには、以下の手順に従います。

1 「**使用するアンテナ**」を設定します。既定値は**最良**です。

2 ドロップダウン メニューから、電波出力を選択します。

- 「**最大出力**」は、最も強い信号を WLAN に送信します。例えば、建物間で信号を送信する場合は、「**最大出力**」を選択します。
- 「**1/2 出力 (-3 dB)**」は、同じビル内のオフィス間に推奨されます。
- 「**1/4 出力 (-6 dB)**」は、短距離の通信に推奨されます。
- 「**1/8 出力 (-9 dB)**」は、比較的短距離の通信に推奨されます。
- 「**最低出力**」は、非常に短い距離の通信に推奨されます。

3 「**断片化のしきい値 (バイト)**」を指定します。最小値は **256**、最大値は **2346** です。既定値は最大値です。

4 「**RTS しきい値 (バイト)**」を設定します。最小値は **1** で、最大値は **2346** です。既定値は最大値です。

5 「**適用**」を選択して設定を保存します。

「**既定の設定への復旧**」をクリックすると、工場出荷時の既定の設定に復旧します。

アクセス ポイントとステーション

802.11 プロトコルを通じて 2 つ以上のホストが接続される場合で、接続を確立するには距離が遠すぎる場合、無線リピータがその間をブリッジします。

SonicWall セキュリティ装置は、アクセス ポイント モードとブリッジ モードがあります。「**アクセス ポイントとステーション**」モードで動作中は、1 つの仮想アクセス ポイントがステーションとして作成されて、別のアクセス ポイントに接続できます。他の仮想アクセス ポイントは通常のアクセス ポイントとして動作します。つまり、装置を「**アクセス ポイントとステーション**」に設定すると、リピーターモードで動作します。このモードでは、仮想アクセス ポイントが WAN インターフェースとして使用する仮想インターフェースを設定することもできます。

無線配信システム (WDS) を使うと、複数のアクセス ポイントを接続できるようになります。WDS では、標準的な形の配線を使わずにアクセス ポイントどうしが通信します。この機能は、ローミング クライアントにシームレスな使用環境を提供し、複数の無線ネットワークを管理するうえできわめて重要です。また、この機能により、必要な配線の量を減らしてネットワーク インフラストラクチャを簡素化することもできます。

無線装置をアクセス ポイントとステーションとして設定するには、以下に説明されているオプションを設定してください。

- アクセス ポイントとステーション 無線設定
- アクセス ポイントとステーション 無線仮想アクセス ポイント
- ステーション設定

アクセス ポイントとステーション 無線設定

重要：無線装置をアクセス ポイントとステーションとして設定する場合、無線運用者は、該当する地域の電波を管轄する関係団体または機関により発布されているすべての法令や規制を遵守する責任を負います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 基本設定**」を選択します。

3 「**無線の役割**」フィールドで、「**アクセス ポイントとステーション**」をドロップダウン メニューから選択します。

4 「**WLAN を有効にする**」チェックボックスをオンにします。これによって、モバイル ユーザにクリーンな無線アクセスを提供できます。「**適用**」を選択して設定を有効にします。WLAN 無線は既定では有効になっています。

5 「**スケジュール**」フィールドで、ドロップダウン メニューから WLAN 無線をアクティブにする時間を選択します。スケジュール リストには、システムが提供するオプションに加えて、「**システム セットアップ | 装置 > システム スケジュール**」ページで作成および管理するスケジュール オブジェクトが表示されます。既定値は「**常に有効**」です。

6 「**国番号**」フィールドには、アクセス ポイントが使用される国を選択してください。国番号は、どの利用認可対象地域の管轄で無線を利用するかを決定します。

7 「**WDS AP を有効にする**」チェックボックスをオンにします。WDS クライアントがこのアクセス ポイントに接続できるようにします。

8 「**SSID**」フィールドが正しく入力されているか確認してください。既定値は、**sonicwall-** に BSSID の最後の 4 文字を付加したもの (例: `sonicwall-C587`) になります。SSID は、32 文字以内の任意の英数字に変更できます。

9 「**適用**」を選択して設定を保存します。

アクセス ポイントとステーション 無線仮想アクセス ポイント

無線仮想アクセス ポイントを使用する場合、「**無線仮想アクセス ポイント**」セクションのドロップダウン メニューから「**無線仮想アクセス ポイント グループ**」を選択してください。または、定義済の VAP グループを選択することもできます。

すべてのアクセス ポイント設定が終了したら、「**適用**」を選択して設定を保存します。

ステーション設定

ステーション設定を構成するには、以下の手順に従います。

1 「**ステーション モードを有効にする**」チェックボックスをオンにします。

2 フィールドに **AP SSID** を入力します。

3 ドロップダウン メニューから AP 認証種別を選択します。以下から選択します。

- オープン
- WPA-PSK

- WPA2-PSK

4 ドロップダウン メニューから「**暗号化種別**」を選択します。

5 **事前共有鍵**を入力します。

6 ドロップダウン メニューから「**VLAN ID**」を選択します。

7 **無線インターフェースを WAN として使用する**場合にはチェックボックスをオンにします。

8 **WDS ステーションを有効にす**る場合にはチェックボックスをオンにします。

9 「**適用**」を選択して設定を保存します。

30

無線セキュリティの設定

「**接続 | 無線 > セキュリティ**」ページでは、無線装置の認証と暗号化設定を構成します。選択した認証の種別に応じて、異なるオプションが表示されます。

トピック:

認証について

認証種別は以下のテーブルで説明されています。

認証種別

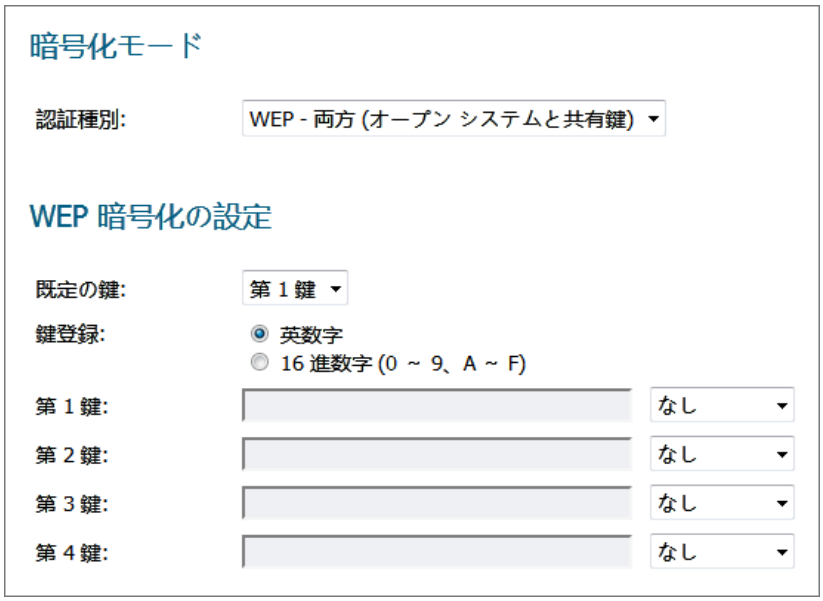
種別	機能と用途
WEP (Wired Equivalent Protocol)	• データを無線ネットワーク経由で保護します。 • SonicWalll 装置を通過後には保護はありません。 • 伝送するデータに対して最小限の保護を提供します。 • 暗号化に静的な鍵を使用します。 • 旧式の機器、PDA、無線プリンタで有用です。 • 高い水準のセキュリティが必要な配備には推奨できません。
WPA (Wi-Fi Protected Access)	• 高いセキュリティ (TKIP を使用) • 信頼性の高い企業の無線クライアントで使用 • Windows ログインを使用したトランスペアレントな認証 • 一般にクライアント ソフトウェアは不要 • RADIUS などのユーザを認証する認証プロトコルが別途で必要です。 • 動的鍵を使用します。 **メモ：**このオプションは、診断ページで有効にした場合のみ表示されます。

認証種別

種別	機能と用途
WPA2 (Wi-Fi Protected Access, v2)	• 最高のセキュリティ (AES を使用) • 信頼性の高い企業の無線クライアントで使用 • Windows ログインを使用したトランスペアレントな認証 • 場合によってクライアント ソフトウェアをインストールする必要がある • 802.11i WPA/WPA2 EAP 認証モードをサポートします。 • 最初のログイン後のバックエンド認証はなし (より高速なローミングが可能) • 鍵の保存と生成に関して 2 つのプロトコルをサポートします。PSK (事前共有鍵) 拡張認証プロトコル (EAP) です。 **メモ**：EAP のサポートは、アクセス ポイント モード (「**接続 | 無線 > 基本設定**」ページで選択) においてのみ使用できます。ブリッジ モードでは使用できません。
WPA2-AUTO	• WPA2 セキュリティを使用して接続を試みる • クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。

WEP 設定の構成

認証種別として WEP オプションの 1 つが選択されている場合、以下のオプションを設定できます。



無線装置に WEP 認証を設定するには、以下の手順に従います。

1 「**接続 | 無線 > セキュリティ**」ページに移動します。

2 「**認証種別**」ドロップダウン メニューで、適切な認証種別を選択します。

- **WEP - 両方 (オープン システムと共有鍵)**(既定)各フィールドで同一の鍵を使用している場合、「**既定の鍵**」の割り当ては重要ではありません。

- 「**WEP - オープン システム**」: オープンシステム認証では、ファイアウォールは ID を検証しないで無線クライアントのアクセスを許可します。すべての Web 暗号化設定は、グレー表示されて選択できません。
- 「**WEP - 共有鍵**」: WEP を使用し、認証を許可する前に無線クライアントに共有鍵が配布されている必要があります。「**共有鍵**」を選択した場合は、「**既定の鍵**」の割り当てが重要です。

3 「**既定の鍵**」ドロップダウン メニューで、既定にする鍵として、「**第 1 鍵**」、「**第 2 鍵**」、「**第 3 鍵**」、または「**第 4 鍵**」を選択します。

4 「**鍵登録**」オプションで、鍵が「**英数字**」か「**16 進数字**」かを選択します。

5 鍵は、指定されたフィールドに 4 つまで入力できます。各鍵について、**64 ビット**、**128 ビット**、**152 ビット**のいずれかを選択します。ビット数が多いほど、鍵は安全になります。個々の種別の鍵について、何文字が必要かについては以下のテーブルを参照してください。

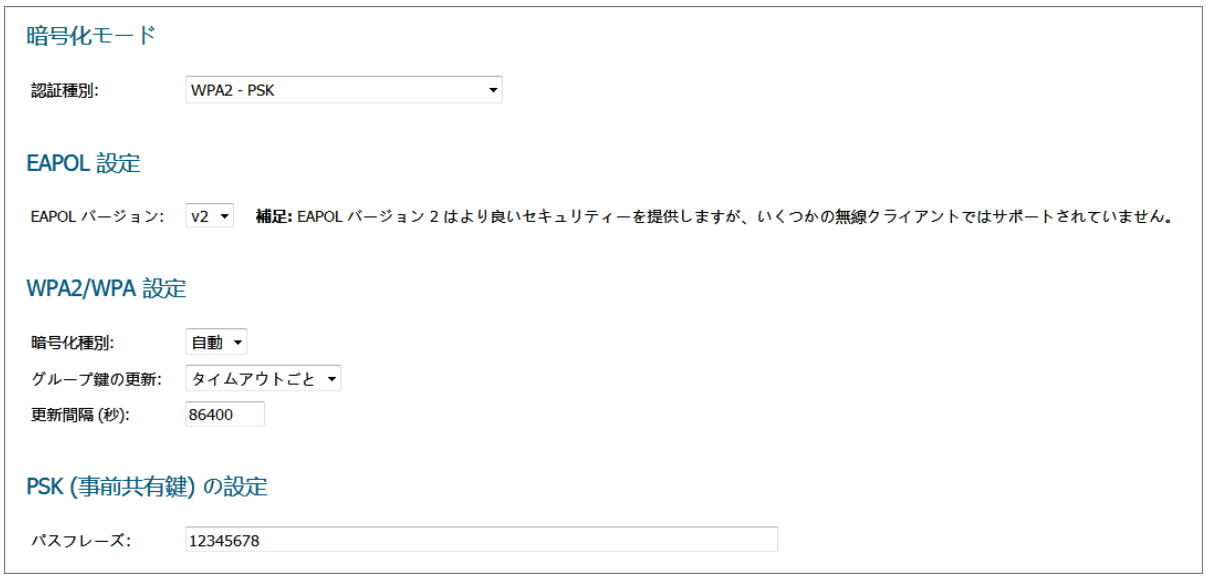
鍵種別

鍵種別	WEP - 64 ビット	WEP - 128 ビット	WEP - 152 ビット
英数字	5 文字	13 文字	16 文字
16 進数字 (0 ～ 9、A ～ F)	10 文字	26 文字	32 文字

6 「**適用**」を選択します。

WPA2 PSK と WPA PSK の設定

認証種別として WPA PSK オプションの 1 つが選択されている場合、以下のオプションを設定できます。



無線装置に設定済の共通鍵を使用する WPA 認証を設定するには、以下の手順に従います。

1 「**接続 | 無線 > セキュリティ**」ページに移動します。

2 「**認証種別**」ドロップダウン メニューで、適切な認証種別を選択します。

- **WPA2 - PSK**: WPA2 と設定済認証鍵を使用して接続します。

- **WPA2 - 自動 - PSK**: 自動的に WPA2 と設定済認証鍵を使用しての接続を試行し、クライアントが WPA2 に対応していない場合には WPA にフォールバックします。

3 ドロップダウン メニューから「**EAPOL バージョン**」を選択します。

- **V2** (既定) - バージョン 2 を選択します。バージョン 1 よりセキュリティは強化されますが、無線クライアントによってはサポートしていない場合があります。
- **V1** (既定) - バージョン 1 を選択します。

4 「**WPA2/WPA 設定**」セクションで、以下の設定を指定してください。

- **暗号化種別** - TKIP を選択します。*Temporal Key Integrity Protocol* (TKIP) は、パケット単位で鍵の整合性を適用するためのプロトコルです。ただし、安全性は比較的低く、スループットも下がります。AES と自動も暗号化種別のオプションです。
- 「**グループ鍵の更新**」: SonicWall セキュリティ装置が鍵をいつ更新するかを指定します。秒数で指定した間隔の後で新しいグループ鍵を生成するには、「**タイムアウトごと**」を選択します。これが既定です。静的鍵を使用する場合は「**使用しない**」を選択します。
- **間隔** -「**グループ鍵の更新**」フィールドで「**タイムアウトごと**」を選択した場合は、WPA が新しいグループ鍵を自動的に生成するまでの秒数を入力します。既定値は **86400** 秒です。「**グループ鍵の更新**」で「**無効**」を選択した場合は、このオプションは表示されません。

5 「**パスフレーズ**」フィールドに、鍵の生成に使用するパスフレーズを入力します。

6 「**適用**」を選択して設定を保存して適用します。

WPA2 EAP と WPA EAP の設定

認証種別として WPA EAP オプションの 1 つが選択されている場合、以下のオプションを設定できます。

無線装置に設定済の共通鍵を使用する WPA 認証を設定するには、以下の手順に従います。

1 「**接続 | 無線 > セキュリティ**」ページに移動します。

2 「**認証種別**」ドロップダウン メニューで、適切な認証種別を選択します。

- **WPA2 - EAP**: WPA2 拡張認証プロトコル (EAP) を使用して接続します。
- **WPA2 - 自動 - EAP**: 自動的に WPA2 と拡張認証プロトコルを使用しての接続を試行し、クライアントが WPA2 に対応していない場合には WPA にフォールバックします。

メモ：EAP は、アクセス ポイント モードにおいてのみサポートされています。クライアント ブリッジ モードではサポートされません。

3 ドロップダウン メニューから「**EAPOL バージョン**」を選択します。

- 「**V1**」: LAN バージョン 1 経由の拡張認証プロトコルを選択します。
- 「**V2**」: LAN バージョン 2 経由の拡張認証プロトコルを選択します。バージョン 1 よりセキュリティは強化されますが、無線クライアントによってはサポートしていない場合があります。

4 「**WPA2/WPA 設定**」セクションで、以下の設定を指定してください。

- 「**暗号化種別**」 - TKIP を選択します。*Temporal Key Integrity Protocol* (TKIP) は、パケット単位で鍵の整合性を適用するためのプロトコルです。ただし、安全性は比較的低く、スループットも下がります。AES と自動も暗号化種別のオプションです。
- 「**グループ鍵の更新**」: SonicWall セキュリティ装置が鍵をいつ更新するかを指定します。秒数で指定した間隔の後で新しいグループ鍵を生成するには、「**タイムアウトごと**」を選択します。これが既定です。静的鍵を使用する場合は「**使用しない**」を選択します。
- 「**更新間隔 (秒)**」-「**グループ鍵の更新**」フィールドで「**タイムアウトごと**」を選択した場合は、WPA が新しいグループ鍵を自動的に生成するまでの秒数を入力します。既定値は **86400** 秒です。「**グループ鍵の更新**」で「**無効**」を選択した場合は、このオプションは表示されません。

5 **EAP (拡張認証プロトコル) の設定** セクションでは、以下の設定を指定してください。

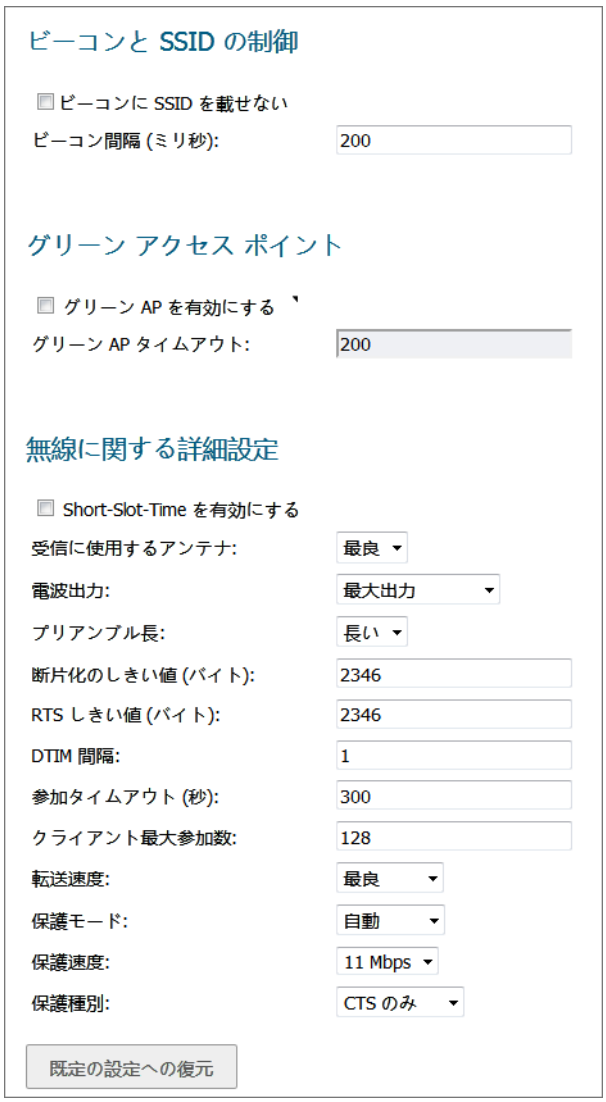
- 「**RADIUS サーバ再試行回数**」: サーバによる認証の試行回数を入力します。既定値は **4** です。
- 「**再試行間隔 (秒)**」: サーバが次の再試行まで待つ時間を入力します。既定値は **0** (間隔を置かない) です。
- 「**RADIUS サーバ 1 IP**」と「**ポート**」: プライマリ RADIUS サーバの IP アドレスとポート番号を入力します。
- 「**RADIUS サーバ 1 事前共有鍵**」: Radius サーバにアクセスするためのパスワードを入力します。
- 「**RADIUS サーバ 2 IP**」と「**ポート**」: セカンダリ RADIUS サーバがある場合は、その IP アドレスとポート番号を入力します。
- 「**RADIUS サーバ 2 事前共有鍵**」: Radius サーバにアクセスするためのパスワードを入力します。

6 「**適用**」をクリックして WPA2 EAP 設定を適用します。

31

無線の詳細設定

詳細設定では、無線装置のための広範囲な機能をカスタマイズできます。このページは、ファイアウォールがアクセス ポイントとして動作している場合にのみ使用できます。



トピック:

ビーコンと SSID の制御

ビーコンと SSID の制御を設定するには:

1 「**管理**」ページに移動します。

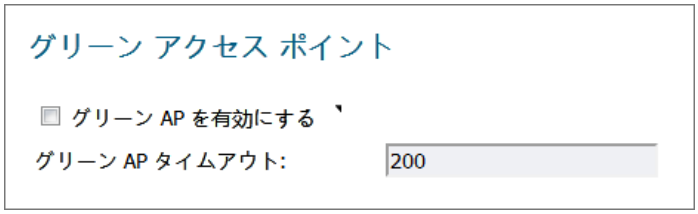
1 「**接続 | 無線 > 詳細設定**」ページに移動します。

2 「**ビーコンに SSID を載せない**」を選択します。これは、SSID 名のブロードキャストを抑止し、プローブ要求への応答を無効にします。このオプションをオンにすると、許可されていない無線クライアントによってその無線 SSID が認識されるのを防ぐことができます。この設定はデフォルトで無効になっています。

3 「**ビーコン間隔 (ミリ秒)**」の値をミリ秒単位で入力します。間隔を短くすると、ビーコン フレームがネットワークを無線接続にいっそう頻繁に通知するので、パッシブ スキャンの信頼性と速度が向上します。既定の間隔は **200** ミリ秒です。

4 適用を選択して変更を適用します。既定の設定に復旧 をクリックすると、工場出荷時の既定の設定に復旧します。

グリーン アクセス ポイント



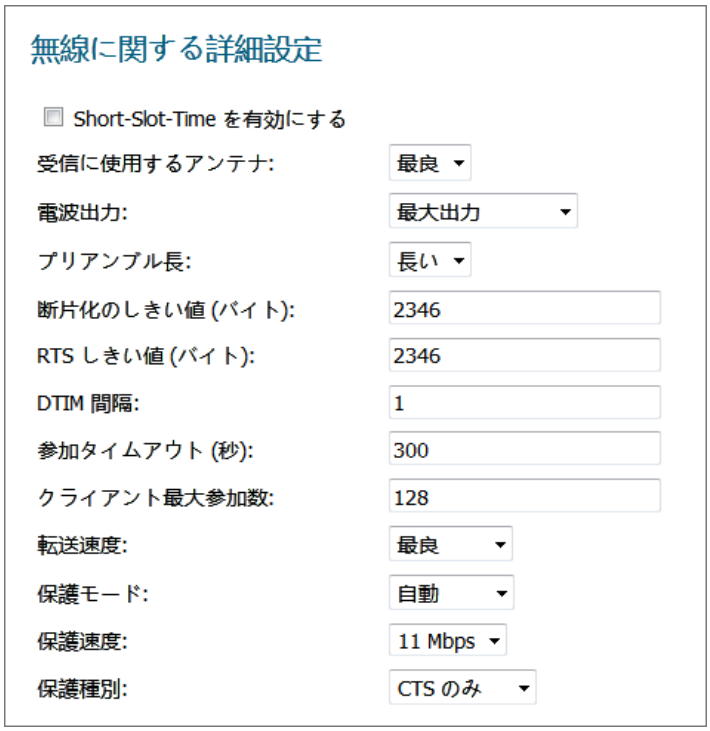
電力効率を設定するには、以下の手順に従います。

1 電力効率を高めるには、「**グリーン AP を有効にする**」を選択します。この設定はデフォルトで無効になっています。

2 「**グリーン AP タイムアウト**」フィールドにタイムアウト時間を指定します。既定値は **200** です。

3 適用を選択して変更を適用します。既定の設定に復旧 をクリックすると、工場出荷時の既定の設定に復旧します。

無線に関する詳細設定



無線に関する詳細設定を行うには、以下の手順に従います。

1 予想されるのが 802.11g トラフィックだけの場合は、「**Short-Slot-Time を有効にする**」を選択するとパフォーマンスが向上します。802.11b は Short-Slot-Time と互換性がありません。この設定はデフォルトで無効になっています。

2 「**受信に使用するアンテナ**」ドロップダウン メニューから、無線セキュリティ装置がデータの送受信に使用するアンテナを選択します。アンテナ選択のより詳細については、「設定可能な使用するアンテナ」を参照してください。既定は「**最良**」です。

3 「**電波出力**」ドロップダウン メニューから、次のいずれかを選択します。

- 「**最大出力**」は、最も強い信号を WLAN に送信します。例えば、建物間で信号を送信する場合は、「**最大出力**」を選択します。
- 「**1/2 出力 (-3 dB)**」は、同じビル内のオフィス間に推奨されます。
- 「**1/4 出力 (-6 dB)**」は、比較的短距離の通信に推奨されます。
- 「**1/8 出力 (-9 dB)**」は、比較的短距離の通信に推奨されます。
- 「**最低出力**」は、非常に短い距離の通信に推奨されます。

4 「**プリアンブル長**」ドロップダウン メニューから、「**短い**」または「**長い**」を選択します。無線ネットワークでの効率化とスループット向上のため、「**短い**」をお勧めします。既定は「**長い**」です。

5 「**断片化のしきい値 (バイト)**」を指定します。最小値は 256、最大値は 2346、既定値は **2346** です。

無線フレームの断片化は、RF 干渉が存在する場所や、無線通信範囲の電波が弱い場所において、信頼性とスループットを向上させます。しきい値が低いほど、より細かく断片化されます。この値を大きくすると、フレームが配信されるときのオーバーヘッドは小さくなりますが、失われたり壊れたりしたフレームは破棄して再送信する必要があります。

6 **RTS しきい値 (バイト)** を、RTC に対して送信するよう依頼します。最小値は 1、最大値は 2347、既定値は **2346** です。

このフィールドには、パケット送信の前に送信する RTS のパケット サイズのしきい値をバイト単位で設定します。RTS を送信すると、クライアントが同じアクセス ポイントの範囲内にあるが互いの範囲内にあるとは限らないという状況で、無線の衝突が生じないようにすることができます。ネットワークのスループットが低い場合、または再送信されるフレームの数が多い場合は、RTS しきい値を小さくして RTS クリーニングを有効にします。

7 DTIM (Delivery of Traffic Indication Message) 間隔を、「**DTIM 間隔**」フィールドに指定します。最小値は 1、最大値は 256、既定値は **1** です。

マルチキャスト パケットを受信する 802.11 省電力モードのクライアントに対し、「DTIM 間隔」は、DTIM を送信する前に待つビーコン フレーム数を指定します。DTIM 間隔の値を大きくすると、電力をいっそう効果的に節約できます。

8 クライアント参加の秒数を、「**参加タイムアウト (秒)**」フィールドに入力します。既定値は **300** 秒で、設定可能な範囲は 60～36000 秒です。ネットワークが非常にビジーの場合、このフィールドの秒数を増やすことによって、タイムアウトを長くできます。

9 このプロファイルを使用する SonicPoint ごとに「**クライアント最大参加数**」を入力します。最小値は 1、最大値は 128、既定値は 128 です。この設定によって、同時に無線接続できるステーションの数が制限されます。

10 「**転送速度**」ドロップダウン メニューから、データが送受信される速度を選択します。「**最良**」では、電磁波妨害やその他の要因を考慮したうえで、その地域で利用できる最適な速度が自動的に選択されます。あるいは、**1 Mbps ～ 54 Mbps** の転送速度を手動で選択することができます。

11 「**保護モード**」ドロップダウン メニューから、保護モードを選択します。「**なし**」、「**常に**」、「**自動**」のいずれかを選択します。

保護により競合を減らすことができます。特に、2 つの SonicPoint が重複している場合に有効です。ただし、パフォーマンスが低下する場合があります。通常は、「**自動**」が最善の設定です。SonicPoint が重複している場合にのみ有効になるためです。

12 「**保護速度**」をドロップダウン メニューから選択します。「**1 Mbps**」、「**2 Mbps**」、「**5 Mbps**」、または「**11 Mbps**」を選択します。保護速度は、保護モードが有効になっているときの転送速度です。速度が遅いほど保護レベルは高くなりますが、データ伝送速度は遅くなります。

13 「**保護種別**」ドロップダウン メニューから、無線接続の確立に使用されるハンドシェイクの種類として、「**CTS のみ**」 (既定) または「**RTS と CTS**」を選択します。

メモ：802.11b トラフィックと互換性があるのは **CTS** だけです。

14 適用を選択して変更を適用します。既定の設定に復旧 をクリックすると、工場出荷時の既定の設定に復旧します。

設定可能な使用するアンテナ

SonicWall 無線セキュリティ装置には、ダイバーシティモードで動作する 5 dBi のデュアルアンテナが採用されています。ダイバーシティモードの既定の実装では、1 つのアンテナが送信用に使用され、両方のアンテナが受信アンテナとして使用できるようになっています。セキュリティ保護された無線装置の両方のアンテナに無線信号が届くと、信号の強度と整合性が評価された後、受信された最善の信号が使用されます。2 つのアンテナの選択処理は動作中は一定であり、常に可能な限り最善の信号が提供されます。外部の (ゲインが高く単一指向性の) アンテナを使用できるよう、使用するアンテナの設定は無効にできます。

SonicWall NSA 220 および 250M 無線セキュリティ装置では、3 つのアンテナが使用されます。「使用するアンテナ」は既定で「**最良**」に設定されており、これらの装置ではこの設定のみを使用できます。

「**使用するアンテナ**」の設定は、無線セキュリティ装置がデータの送受信に使用するアンテナを決定します。規定値の設定は**最良**です。最良を選択すると、強度が最も高く、劣化していない信号を受信したアンテナが無線セキュリティ装置によって自動的に選択されます。

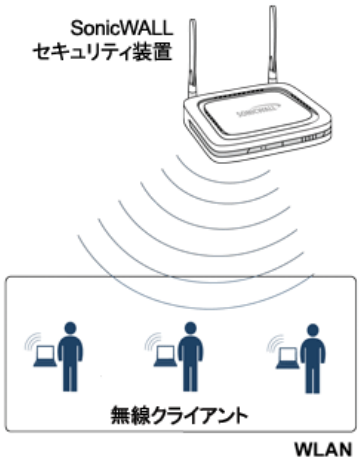
32

無線 > MAC フィルタ リスト

無線ネットワーキングにより、無線セキュリティ装置に対する無線クライアントの認証や参加を防ぐ、ネイティブな MAC フィルタ機能が提供されます。WLAN 上で MAC フィルタを強制すると、無線クライアントは無線ネットワーク カードの MAC アドレスを提出しなければならなくなります。SonicOS 無線 MAC フィルタ リストにより、あなたの無線ネットワークへのアクセスを許可または拒否をするクライアントのリストを設定できます。MAC フィルタリング無しでは、無線ネットワークに入るための SSID および、その他のセキュリティ パラメータを知っていれば、どのような無線クライアントでも無線ネットワークに「押し入る」ことができます。

以下に、一般的な 300 MAC フィルタ リストの配備シナリオを示します。

一般的な SonicWall MAC フィルタ リストの配備



トピック:

- 配備に関して考慮すべき事項
- 無線 > MAC フィルタ リストの設定

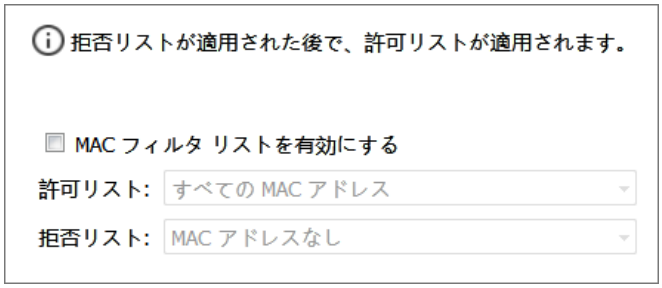
配備に関して考慮すべき事項

MAC フィルタ リストを展開する場合は、以下を考慮します。

- SonicPoint-N 装置の場合、この機能ではゲートウェイが MAC フィルタ リスト設定を保存する必要があります。
- SonicWall TZ シリーズ装置の内部無線の場合、MAC フィルタ リスト設定を保存するために VAP 構造にいくつかメンバーを追加する必要があり、また、ドライバに構成を設定するために機能全体を修正する必要があります。

- 仮想アクセス ポイントは独自の MAC フィルタを設定することもできますし、「**接続 | 無線 > MAC フィルタ リスト**」ページで設定されたグローバル設定を継承することもできます。

無線 > MAC フィルタ リストの設定



MAC フィルタ リストを設定するには、以下の手順に従います。

1 「**管理**」表示を選択します。

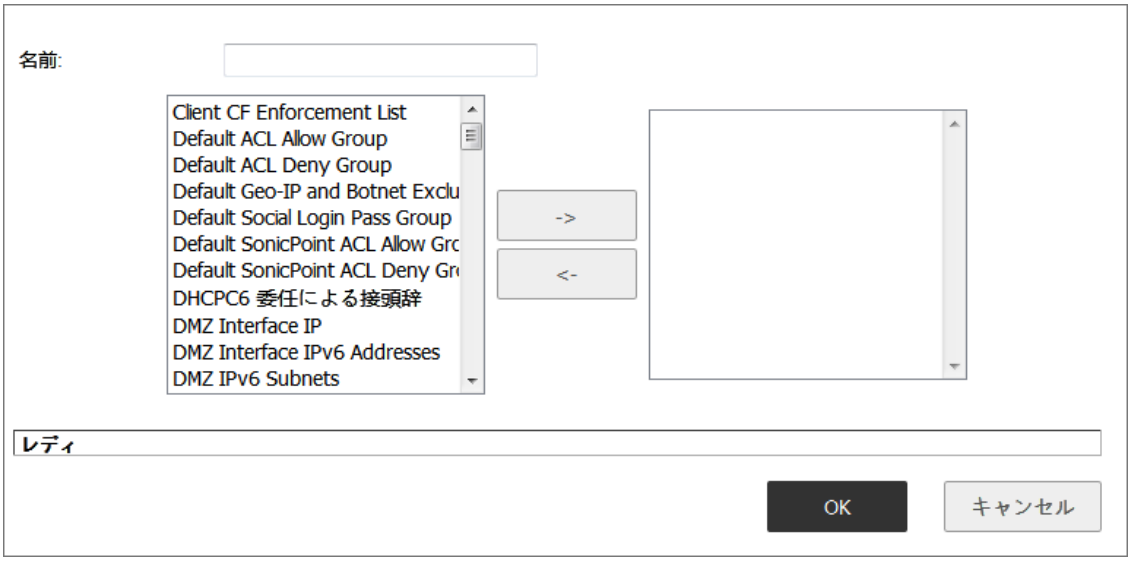
2 「**接続 の 無線 > MAC フィルタ リスト**」を選択します。

3 「**MAC フィルタ リストを有効にする**」チェックボックスをオンにします。この設定はデフォルトで無効になっています。

4 「**許可リスト**」ドロップダウン メニューから、許可したいアドレス グループを選択します。「**すべての MAC アドレス**」(既定)、「**既定 ACL 許可グループ**」、または個別に作成したグループです。

5 「**拒否リスト**」ドロップダウン メニューから、拒否したいアドレス グループを選択します。MAC アドレスなし (既定)、既定 ACL 拒否グループ、または個別に作成したグループです。

6 許可または拒否リストに新しいアドレス オブジェクトを追加するには、「**許可リスト**」または「**拒否リスト**」いずれかのドロップダウン メニューから「**MAC アドレス オブジェクト グループの作成...**」を選択します。



a 「**名前:**」テキスト フィールドに、新しいグループの名前を入力します。

b 左側の列で、許可または拒否するグループあるいは個別のアドレス オブジェクトを選択します。**Ctrl キー**を押すと複数の項目を選択できます。

c 右矢印ボタン「->」を選択して、項目をグループに追加します。

d 「**OK**」を選択します。アドレスが、ドロップダウン メニューの選択肢として表示されます。

e 必要に応じてオブジェクトを選択します。

7 「**適用**」ボタンを選択します。

33

無線 IDS の設定

トピック:

無線 IDS について

無線侵入検知サービス (IDS) を使用すると、SonicWall 無線セキュリティ装置のセキュリティ機能が大幅に向上します。一般的な不正無線アクティビティの大半を認識し、対応策を講じることもできます。無線 IDS は、次の 3 つの種別のサービスで構成されています。

- シーケンス番号分析
- 参加フラッド検出
- 悪意のあるアクセス ポイントの検出

アクセス ポイントの IDS

無線セキュリティ装置の「**無線の役割**」が「**アクセス ポイント**」モードに設定されていると、3 種類の WIDS サービスをすべて使用できますが、Rogue アクセス ポイント検出は既定によりパッシブ モードで機能します (選択されている動作チャンネルのみで他のアクセス ポイント ビーコンのフレームをパッシブにリッスンします)。「**今すぐスキャン**」を選択すると、「無線の役割」が即座に変更されて無線セキュリティ装置はアクティブ スキャンを実行できるようになり、関連する無線クライアントに対する接続がしばらく失われることがあります。「**アクセス ポイント**」モードの間は、アクティブに関連付けられているクライアントがない場合、またはクライアントの接続が中断する可能性があっても問題ない場合にのみ、「**今すぐスキャン**」機能を使用する必要があります。

悪意のあるアクセス ポイント

Rogue (悪意の侵入者) アクセス ポイントは、無線セキュリティに対する最も深刻かつ油断のならない脅威の 1 つです。一般に、ネットワーク上での使用が許可されていないアクセス ポイントは、悪意のあるアクセス ポイントとして認識されます。保護されていないアクセス ポイントの利便性や可用性と、ネットワークへの追加のしやすさによって、Rogue (悪意の侵入者) アクセス ポイントの導入を許す環境が形作られています。具体的には、悪意のある機器への無意識的な接続や、保護されていないチャンネルを介した機密データの転送、LAN リソースへの不要なアクセスなど、多種多様な脅威が生み出されています。これは特定の無線機器のセキュリティ不足ではなく、無線ネットワーク全体のセキュリティの脆弱性を示しています。

セキュリティ装置は、ネットワークへのアクセスを試みる可能性のある Rogue アクセス ポイントを認識することによって、この脆弱性を緩和できます。そのためには、802.11a、802.11g、802.11n チャンネルすべてでのアクセス ポイントのアクティブ スキャンと、単一の動作チャンネルでのビーコン アクセス ポイントの (アクセス ポイント モードでの) パッシブ スキャンという 2 つの方法が使用されます。

IDS の設定

トピック:

- IDS 設定
- 検出されたアクセス ポイント

IDS 設定

IDS スキャンの実行をスケジュールするには、「**IDS スキャンを予定する**」ドロップダウン メニューから、スケジュールを選択または作成します。

- **無効**

  このオプションは既定の設定です。選択すると、IDS スキャンは行われません

- **新しいスケジュールを作成する...**

  「**スケジュールの追加**」ダイアログが表示され、このセクションで説明する個別のスケジュールを作成できます。

- **勤務時間**
- **月-火-水-木-金 08:00 から 17:00**
- **時間外**
- **月-火-水-木-金 0:00 から 8:00**
- **月-火-水-木-金 17:00 から 24:00**
- **土-日 00:00 から 24:00**
- **週末時間**

「IDS スキャンをスケジュールする」ドロップダウン メニューに新しいスケジュールを追加するには、以下の手順に従います。

1 「**IDS スキャンをスケジュールする**」フィールドで、**新しいスケジュールの作成...を選択します。**

2 「**スケジュール名**」を入力します。

3 スケジュール種別で、次のいずれかを選択します。

- 「**1 回**」では、1 回だけのイベントをスケジュールします。「**1 回**」セクションのフィールドだけが入力可能になります。
- 「**繰り返し**」では、繰り返しイベントをスケジュールします。「**繰り返し**」セクションのフィールドだけが入力可能になります。
- 「**混在**」では、混在イベントをスケジュールします。すべてのフィールドが入力可能になります。

4 「**1 回**」セクションでは、ドロップダウン メニューを使用して IDS スキャンの開始と終了の時刻をスケジュールします。

5 「**繰り返し**」セクションで、以下の操作を行います。

a スキャンの「**曜日**」を選択します。

b 24 時間形式で「**開始時刻**」を入力します。

c 24 時間形式で「**終了時刻**」を入力します。

d 「**追加**」をクリックして、これらのパラメータをスケジュール リストに追加します。

e リストから項目を削除するには、反転表示させて「**削除**」をクリックします。「**すべて削除**」をクリックすると、スケジュール リストがクリアされます。

6 「**OK**」を選択して、スケジュールをドロップダウン リストに追加します。

検出されたアクセス ポイント

アクティブ スキャンは、無線セキュリティ装置の起動時、およびテーブルの下部にある「**今すぐスキャン**」がクリックされるたびに、実行されます。装置は環境をスキャンして、近辺にある他の無線デバイスを特定します。テーブルの上の「**補足**」には、検出されたアクセス ポイント数と、最後のスキャンからの経過時間が、日数、時間数、分数、秒数で表示されます。

「**検出されたアクセス ポイント**」テーブルのエントリを更新するには、「**再表示**」を選択します。直ちにスキャンを実行するには、「**今すぐスキャン**」 (テーブルの下部) を選択します。

重要：アクセス ポイント モードで動作している時に「**今すぐスキャン**」機能を使用すると、サービスがしばらく中断します。この中断は次のようなものです。

- 非永続的で処理状態を把握しないプロトコル (HTTP など) には悪影響を及ぼしません。
- 永続的な接続 (FTP などのプロトコル) の場合は、接続状態が悪くなるか、切断されます。

それが問題になる場合は、アクティブなクライアントがなくなるまで、または中断する可能性があってもかまわないときまで待ってから、「**今すぐスキャン**」機能を使用してください。

無線セキュリティ装置がブリッジ モードで動作しているときは、「**今すぐスキャン**」機能を使用してもブリッジされている接続が中断することはありません。

設定

「**検出されたアクセス ポイント**」の表には、すべての SonicPoint または個別の SonicPoint で検出できるすべてのアクセス ポイントについての情報が表示されます。

- **MAC アドレス (BSSID)**: 検出されたアクセス ポイントの無線インターフェースの MAC アドレスです。
- **SSID**: アクセス ポイントの無線 SSID です。
- **チャンネル**: アクセス ポイントで使用される無線チャンネルです。
- **認証**: 認証の種別です。
- **暗号**: 使用する暗号です。
- **ベンダー**: アクセス ポイントの製造元です。SonicPoint で示される製造元は SonicWall と Senao のどちらかです。
- **信号強度**: 検出された無線信号の強度です。
- **最大速度**: アクセス ポイントの無線で利用できる最高転送速度です。通常は 54 Mbps です。
- **許可**: 許可されたアクセス ポイントのアドレス オブジェクト グループにアクセス ポイントを追加するには、「**許可**」列の アイコンを選択します。

ネットワークでのアクセス ポイントの許可

無線セキュリティ装置によって検出されたアクセス ポイントは、動作を許可できるものとして無線セキュリティ装置により識別されるまでは、Rogue (悪意の侵入者) とみなされます。アクセス ポイントを承認するには、**承認**アイコンをクリックしてください。

34

内部ワイヤレス無線機を備えた仮想アクセス ポイントの設定

仮想アクセス ポイント (VAP) とは、単一の物理アクセス ポイントを多重インスタンス化したものです。それ自身を複数の別個なアクセス ポイントとして見せます。無線 LAN クライアントからは各仮想 AP が個別の物理 AP のように見えますが、実際には 1 つの物理 AP しか存在しません。仮想アクセス ポイントでは、単一の物理インターフェース上で複数の個別設定をセットアップすることにより、無線ユーザ アクセスとセキュリティの設定を制御できます。これらの個別設定は、それぞれ別々の (仮想) アクセス ポイントとして機能し、またグループ化して、単一の内部ワイヤレス無線機に適用することができます。

VAP を使用する利点は、以下のとおりです。

- **無線チャンネルの節約** - チャンネルの競合を避けて単一の物理アクセス ポイントをさまざまな目的に使用できるようにすることで、重複したインフラストラクチャの構築を防止します。空港などの公共スペースでは、複数のプロバイダが標準になりつつあります。空港内では、FAA ネットワーク、1 つ以上の航空会社ネットワーク、そして 1 つ以上の無線 ISP をサポートする必要があるかもしれません。けれども、米国とヨーロッパでは 802.11b ネットワークで 3 つの使用可能な (重複していない) チャンネルしかサポートできませんし、フランスと日本では 1 つのチャンネルしか使用できません。それらのチャンネルが既存のアクセス ポイントで利用されてしまえば、追加のアクセス ポイントはお互いに干渉し合い、パフォーマンスが落ちることになります。VAP は単一のネットワークを多様な目的に使用できるようにすることで、チャンネル数を節約します。
- 「**無線 LAN インフラストラクチャの最適化**」- 重複したインフラストラクチャを構築せずに、複数のプロバイダの間で同じ無線 LAN インフラストラクチャを共有することにより、WLAN の設置と保守にかかる費用を引き下げます。

トピック:

無線仮想 AP 設定タスク リスト

無線 VAP を配備するには、いくつかのステップから成る設定手順を実行する必要があります。このセクションでは、以下のステップの概要を説明します。

1 **ネットワーク ゾーン** - ネットワーク ゾーンは VAP 設定の重要部分です。作成した各ゾーンは、それぞれの個別的なセキュリティ設定とアクセス制御設定を持つことになります。複数のゾーンを作成し、無線サブネットを通じて単一の物理インターフェースに適用することができます。ネットワーク ゾーンの詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > ゾーン**」のセクションを参照してください。

2 **無線インターフェース** - W0 インターフェース (およびその WLAN サブネット) は SonicWall ネットワーク セキュリティ装置と内部ワイヤレス無線機の間の物理接続を表します。個々のゾーン設定はこれらのインターフェースに適用され、それからワイヤレス無線機に転送されます。無線インターフェースの詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > インターフェース**」のセクションを参照してください。

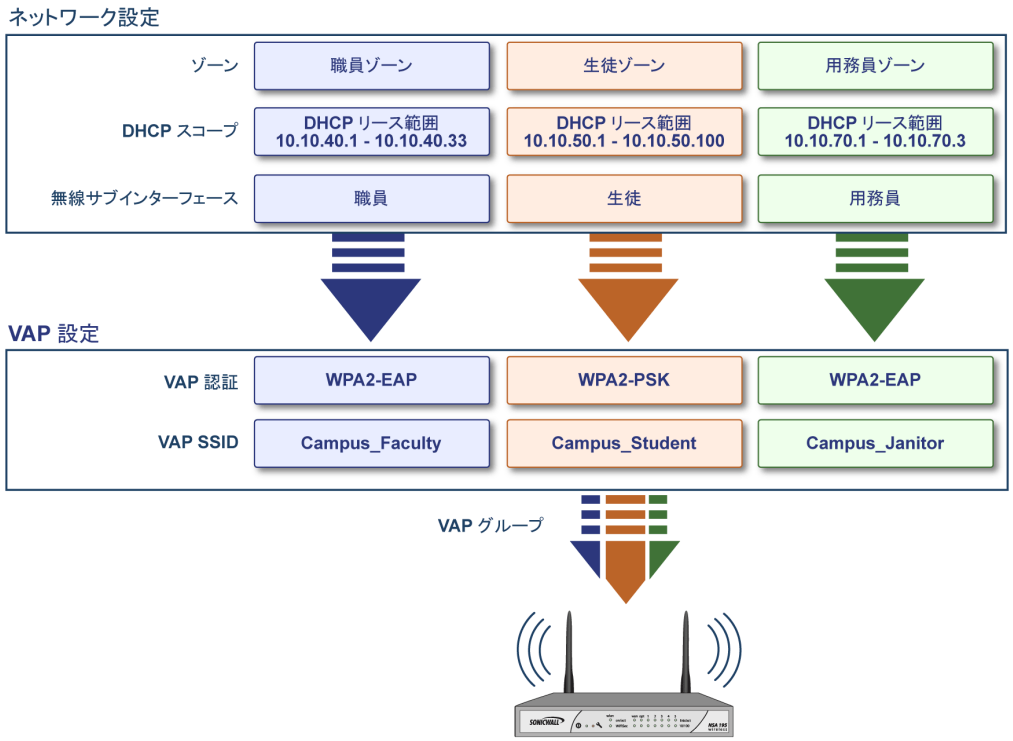
3 **DHCP サーバ** - DHCP サーバはリースされる IP アドレスを指定された範囲 (「*スコープ*」と呼ばれる) 内のユーザに割り当てます。DHCP 対象の既定の範囲は、たいていの無線配備のニーズにとって過大なものです。例えば、30 個のアドレスしか使用しないインターフェースに対して 200 個のアドレスというスコープなど。そのため、利用可能なリース スコープを使い果たさないように、DHCP 範囲は気をつけて設定する必要があります。DHCP サーバ設定の詳細については、「*SonicOS 6.5 システム設定*」の「**管理 | ネットワーク > DHCP サーバ**」のセクションを参照してください。

4 **仮想アクセス ポイント プロファイル** - VAP プロファイル機能では、必要に応じて新しい無線仮想アクセス ポイントに簡単に適用できる無線設定プロファイルを作成できます。詳細については、「**仮想アクセス ポイント プロファイル**」を参照してください。

5 **仮想アクセス ポイント** - VAP オブジェクト機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および無線サブネット名が設定されます。詳細については、「仮想アクセス ポイント」を参照してください。

6 **仮想アクセス ポイント グループ** - VAP グループ機能では、単一の内部ワイヤレス無線機に同時に適用する複数の VAP オブジェクトをグループ化することができます。詳細については、「仮想アクセス ポイント グループ」を参照してください。

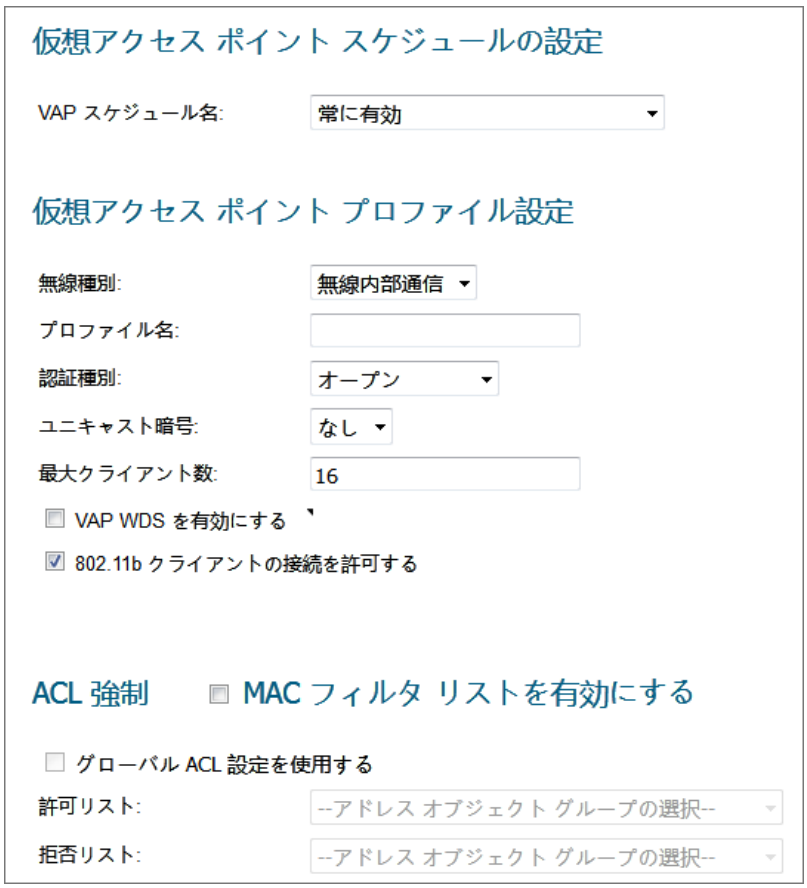
7 **VAP グループを内部ワイヤレス無線機に割り当てる** - VAP グループが内部ワイヤレス無線機に適用され、複数の SSID を通じてユーザが使用可能になります。詳細については、「仮想アクセス ポイント グループの有効化」を参照してください。



仮想アクセス ポイント プロファイル

仮想アクセス ポイント プロファイルを使用すると、アクセス ポイント設定をあらかじめ設定して、プロファイルに保存することができます。VAP プロファイルにより、新しい仮想アクセス ポイントに簡単に設定を適用することができます。仮想アクセス ポイント プロファイルの設定は「**管理 | 無線 > 仮想アクセス ポイント**」ページで行います。プロファイル名を選択して **編集** アイコンを選択するか、「**追加**」を選択して新しい仮想アクセス ポイント プロファイルを作成します。完了したら「OK」を選択します。

ヒント：この機能は、複数の仮想アクセス ポイントが同じ認証方法を共有する場合にすばやく設定を行ううえで特に便利です。



トピック:

- 仮想アクセス ポイント スケジュールの設定
- 仮想アクセス ポイント プロファイルの設定
- ACL 強制

仮想アクセス ポイント スケジュールの設定

個々の仮想アクセス ポイントは固有のスケジュールを持つことができます。拡張により、個々のプロファイルも専用に定義されたスケジュール設定を持つことができます。

スケジュールを仮想アクセス ポイント プロファイルに関連付けるには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して**編集**アイコンをクリックします。

4 「**VAP スケジュール名**」フィールドで、スケジュールをドロップダウン メニューから選択します。

仮想アクセス ポイント プロファイルの設定

仮想アクセス ポイント プロファイルを設定するには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して**編集**アイコンをクリックします。

4 「**無線種別**」を設定します。既定では「**無線内部通信**」になります。VAP アクセスに内部無線機を使用する場合は、既定値のままにしておいてください (これが現在サポートされている唯一の無線種別です)。

5 「**プロファイル名**」フィールドに、この仮想アクセス ポイント プロファイルのわかりやすい名前を入力します。後でこのプロファイルを新しい VAP に適用するときにわかりやすく、覚えやすい名前にするとよいでしょう。

6 「**認証種別**」をドロップダウン リストから選択します。以下のオプションから選択します。

認証種別	定義
オープン	認証方法を特定しない
共有	WEP 暗号化認証設定では、共有鍵が使用されます。
両方	共有鍵が設定されていなければ、公開ネットワークと同じです。 共有鍵が設定されていれば、公開認証でデータ トラフィックは暗号化されていることになります。
WPA2-PSK	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。認証に事前共有鍵を使います。
WPA2-EAP	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。拡張認証プロトコル (EAP) を使用します。
WPA2 - 自動 - PSK	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。認証には事前共有鍵を使用します。
WPA2 - 自動 - EAP	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。拡張認証プロトコル (EAP) を使用します。

選択された認証種別に基づいて、「**ユニキャスト暗号**」フィールドが表示されます。

メモ：ページに表示される設定は、選択したオプションに応じて異なります。

7 「**最大クライアント数**」フィールドには、この仮想アクセス ポイントに対して許容される同時クライアント接続の最大数を選択します。

8 「**VAP WDS を有効化する**」 (無線配信システム) のチェックボックスをオンにします。既定では、このオプションはオフになっています。

9 「**802.11b クライアントの接続を許可する**」チェックボックスをオンにします。既定では、このオプションは選択されています。

選択された「**認証種別**」に応じて、仮想 アクセス ポイント プロファイルの追加/編集ページには、追加のオプションのセクションが表示されます。

- 「**両方**」または「**共有**」を選択した場合の設定の情報については、「WEP 暗号化の設定」を参照してください。
- 事前共有鍵 (PSK) を必要とするオプションを選択した場合の設定の情報については、「WPA-PSK > WPA2-PSK 暗号化の設定」を参照してください。
- 拡張認証プロトコル (EAP) を使用するオプションを選択した場合の設定の情報については、「WPA-EAP > WPA2-EAP 暗号化の設定」を参照してください。

WEP 暗号化の設定

前の手順のステップ 6 で「**両方**」または「**共有**」を選択した場合、「**WEP 暗号化設定**」と呼ばれる設定が表示されます。WEP 設定は、物理アクセス ポイントを共有する仮想アクセス ポイント間で共有されます。

「**暗号化鍵**」フィールドで、「**第 1 鍵**」、「**第 2 鍵**」、「**第 3 鍵**」、または「**第 4 鍵**」をドロップダウン リストから選択します。

WPA-PSK > WPA2-PSK 暗号化の設定

ステップ 6 で、事前共有鍵が必要なオプション - 「**WPA2-PSK**」または「**WPA2-自動-PSK**」 - を選択した場合、「**WPA/WPA2-PSK 暗号化設定**」と呼ばれる設定が表示されます。これらの設定が定義されると、事前共有鍵が認証に使用されます。以下のフィールドに値を入力します。

フィールド名	説明
パスフレーズ	PSK ベースの認証で接続するときにユーザが入力する共有パスフレーズ
グループ鍵間隔	グループ鍵が有効な時間間隔。既定値は 86400 秒です。この値を小さく設定すると、接続の問題が生じる可能性があります。

WPA-EAP > WPA2-EAP 暗号化の設定

ステップ 6 で、EAP が必要なオプション - 「**WPA2-EAP**」または「**WPA2-自動-EAP**」- を選択した場合、「**RADIUS サーバ設定**」と呼ばれる設定が表示されます。この設定が定義されると、鍵の生成および認証に外部の 802.1x/EAP 対応 RADIUS サーバを利用します。以下のフィールドに値を入力します。

フィールド名	説明
RADIUS サーバ再試行回数	アクセスを拒否するまでにユーザが認証を試行できる回数を入力します。既定値は 4 です。
再試行間隔 (秒)	再試行が有効な期間を入力します。既定値は 0 です。
RADIUS サーバ 1	RADIUS 認証サーバの名前/場所を入力します。
ポート	プライマリ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポートを入力します。
RADIUS サーバ 1 事前共有鍵	プライマリ RADIUS サーバ用のシークレット パスコードを入力します。
RADIUS サーバ 2	バックアップ RADIUS 認証サーバの名前/場所を入力します。
ポート	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク機器と通信するポートを入力します。
RADIUS サーバ 2 事前共有鍵	バックアップ RADIUS 認証サーバ用のシークレット パスコードを入力します。
グループ鍵間隔	WPA/WPA2 グループ鍵が更新される時間間隔 (秒数) を入力します。既定値は 86400 です。

ACL 強制

各仮想アクセス ポイントは、個別のアクセス制御リスト (ACL) をサポートして、より効率的な認証制御を提供できます。この無線 ACL 拡張機能は、現在 SonicOS で利用可能な無線 MAC フィルタ リストと同時に動作します。この ACL 強制機能を使って、ユーザは MAC フィルタ リストを有効/無効にする、許可リストを設定する、そして拒否リストを設定することが可能です。

各 VAP は個別の MAC フィルタ リスト設定を持つ、またはグローバル設定を使うことが可能です。仮想アクセス ポイント (VAP) モードでは、このグループの各 VAP が同一 MAC フィルタ リスト設定を共有します。

MAC フィルタ リストの強制化を有効にする

1 「**MAC フィルタ リストを有効にする**」チェックボックスをオンにします。MAC フィルタ リストが有効な場合、他の設定項目も設定できるように表示されます。

2 「**グローバル ACL 設定を使用する**」場合にはチェックボックスをオンにします。これによって、仮想アクセス ポイントに、SonicWall ネットワーク セキュリティ装置の既存の MAC フィルタ リスト設定が関連付けられます。このオプションを有効にした場合は、許可/禁止リストを編集できなくなることに注意してください。

3 「**許可リスト**」で、ドロップダウン リストからオプションを選択します。どの MAC アドレスにアクセスを許可するかを指定します。

アクセスさせたい MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。これを行うための情報については、「*SonicOS 6.5 ポリシー*」を参照してください。

4 「**拒否リスト**」で、ドロップダウン リストからオプションを選択します。どの MAC アドレスからのアクセスを拒否するかを指定します。

アクセスさせたくない MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。これを行うための情報については、「*SonicOS 6.5 ポリシー*」を参照してください。

5 完了したら「**OK**」を選択します。

仮想アクセス ポイント

VAP 設定機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および無線サブネット名が設定されます。仮想アクセス ポイントの設定は、「**管理**」表示の「**接続 | 無線 > 仮想アクセス ポイント**」ページで行います。

トピック:

- VAP 一般設定
- VAP 詳細設定

VAP 一般設定

仮想アクセス ポイントの一般設定は、以下の手順に従ってください。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 既存の仮想アクセス ポイントの設定を編集するには、そのアクセス ポイントに対する**編集**アイコンを選択します。新しいアクセス ポイントを作成するには、「**仮想アクセス ポイント プロファイル**」セクションの「**追加**」ボタンをクリックします。

4 「**名前**」フィールドにアクセス ポイントのわかりやすい名前を入力します。

5 「**SSID**」フィールドに一意の名前を入力します。この名前は、パケット ヘッダーに添付される一意の識別子になります。最大 32 文字の英数字で、大文字と小文字は区別されます。

6 ドロップダウン メニューから **VLAN ID** を選択します。

7 「**仮想アクセス ポイントを有効にする**」チェックボックスをオンにします。

8 必要に応じて、権限のない無線クライアントから無線 SSID を確認できなくする場合は、「**SSID 抑制を有効にする**」チェック ボックスをオンにします。オンにした場合、SSID 名のブロードキャストを抑止し、プローブ要求への応答を無効にします。

9 「**OK**」を選択します。

VAP 詳細設定

「**詳細設定**」では、仮想アクセス ポイントの認証と暗号化が設定できます。表示されるオプションは、仮想アクセス ポイント プロファイルを定義した時と同じです。

仮想アクセス ポイントの詳細設定は、以下の手順に従ってください。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 既存の仮想アクセス ポイントの設定を編集するには、そのアクセス ポイントに対する**編集**アイコンを選択します。新しいアクセス ポイントを作成するには、「**仮想アクセス ポイント プロファイル**」セクションの「**追加**」ボタンをクリックします。

4 「**詳細設定**」を選択します。

5 「**仮想アクセス ポイントの詳細設定**」の見出しで、「**プロファイル名**」をドロップダウン リストから選択します。そのプロファイルのすべての設定が、プロファイルから自動で入力されます。

プロファイルを使用しない場合、「**プロファイル名**」を「**プロファイルを使用しない**」のままにして、「仮想アクセス ポイント プロファイル」の説明に従って残りのフィールドに入力します。

6 「**OK**」を選択します。

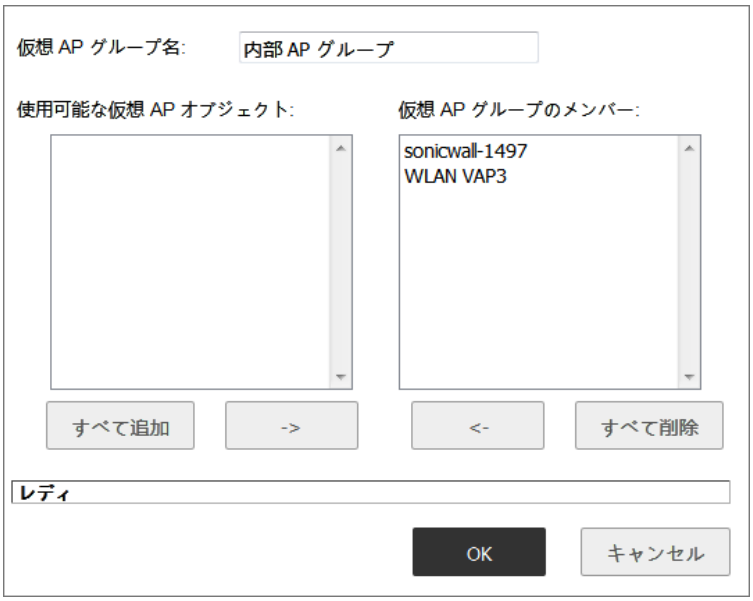
仮想アクセス ポイント グループ

仮想アクセス ポイント グループ機能では、単一の内部ワイヤレス無線機に適用する複数の VAP オブジェクトをグループ化することができます。仮想アクセス ポイント グループの設定は、「**管理**」表示の「**接続 | 無線 > 仮想アクセス ポイント**」で行います。

メモ：仮想アクセス ポイント グループを作成するには、複数の仮想アクセス ポイントが設定されていることが必要です。アクセス ポイントが 1 つしかない場合、自動的に既定のグループである内部 AP グループに追加されます。

仮想アクセス ポイント グループの有効化は、以下の手順に従います。

1 「**管理**」表示を選択します。
2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。
3 既存の仮想アクセス ポイント グループの設定を編集するには、そのアクセス ポイントに対する**編集**アイコンを選択します。



4 オブジェクトをグループに追加するには、「**使用可能な仮想 AP オブジェクト**」リストから追加したいオブジェクトを選択して、右矢印をクリックしてください。
5 グループからオブジェクトを削除するには、「**仮想 AP グループ メンバー**」リストからオブジェクトを選択し、左矢印ボタンを選択します。
6 完了したら「**OK**」を選択します。

仮想アクセス ポイント グループの有効化

仮想アクセス ポイントを設定して VAP グループに追加した後、そのグループを内部無線に適用してユーザが利用可能にしなくてはなりません。

グループを利用可能にするには、以下の手順に従います。

1 「**管理**」表示を選択します。
2 「**接続**」で「**無線 > 基本設定**」を選択します。
3 「**無線仮想アクセス ポイント**」まで画面をスクロールします。
4 「**仮想アクセス ポイント グループ**」フィールドで、ドロップダウン メニューから「**内部 AP グループ**」を選択します。
5 「**適用**」を選択して設定を更新します。

第 5 部

接続性 | 3G/4G/モデム

- 3G/4G/モデム概要
- 3G/4G/モデム基本設定の設定
- 3G/4G/モデム詳細設定の構成
- 3G/4G/モデムの接続プロファイルの設定
- 3G/4G データ転送の監視

35

3G/4G/モデム概要

USB 拡張ポートを備えた SonicWall ネットワーク セキュリティ装置は、外部の 3G/4G/LTE インターフェースまたはアナログ モデム インターフェースのどちらかをサポートできます。

トピック:

デバイスの検知とインターフェースの選択

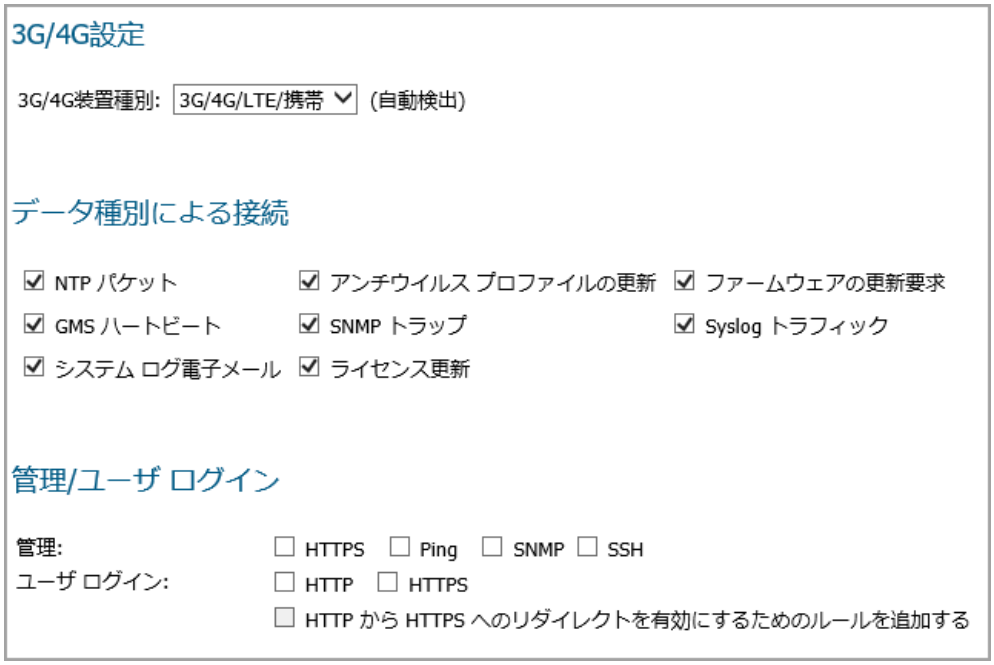
既定動作として、装置は接続されている外部機器の種別を検知しようとします。種別を特定することに成功した場合、左側のナビゲーションの表示が検知されたものに変わります。

設定するインターフェースの種別を「**接続 | 3G/4G/モデム > 基本設定**」ページで手動で指定できます。

「**3G/4G/モデム装置種別**」ドロップダウン メニューには次のオプションが用意されています。

- 「**自動検出**」- どのような機器が接続されたかの判断を装置が試みます。
- 「**3G/4G/LTE/モバイル**」- 3G/4G/LTE/モバイル インターフェースを手動で設定します。
- 「**アナログ モデム**」- アナログ モデム インターフェースを手動で設定します。

検知または識別されたデバイスがその後に接続されると、「**接続 | 3G/4G/モデム > 基本設定**」ページにその構成設定が表示されます。



メモ：3G/4G/LTE デバイスは、U0 インターフェースの「**管理**」ボタンを選択した後に、「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページから接続/切断できます。「U0/U1 インターフェースを有効にする (321 ページ)」を参照してください。

3G/4G/LTE について

SonicWall セキュリティ装置は、セルラー ネットワークを介したデータ接続を利用する 3G/4G/LTE 無線 WAN 接続をサポートしています。3G/4G/LTE 接続は次の用途に使用できます。

- 電線やケーブルに依存しない接続を使用する WAN フェイルオーバー。
- 見本市やキオスクなど、事前設定した接続を利用できない一時的なネットワーク。
- 車両内に SonicWall 装置を設置した場合のモバイル ネットワーク。
- 有線接続は利用できないが、3G/4G セルラーを利用できるプライマリ WAN 接続。

3G/4G インターフェースを使用するには、3G/4G/LTE PC カードが必要です。また、無線サービス プロバイダと契約を結ぶ必要があります。サポートされているハードウェアの可用性を第一に考慮して 3G/4G/LTE サービス プロバイダを選択してください。SonicOS がサポートする機器のリストについては、次のサイトを参照してください。
https://www.sonicwall.com/ja-jp/support/knowledge-base/170505473051240

SonicOS では、次の 3G/4G/LTE 無線ネットワーク プロバイダがサポートされています (このリストは変更されることがあります)。

- AT&T
- China Telecom
- H3G
- Telefonica
- T-Mobile
- TDC Song

- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile
- Verizon Wireless
- Vodaphone

トピック:

- 3G/4G/LTE 接続種別
- SonicWave MiFi Extender
- 3G/4G/LTE フェイルオーバー

3G/4G/LTE 接続種別

3G/4G/LTE 機器が装着されている状態で装置を起動した場合は、「**管理**」表示で「**システム セットアップ > ネットワーク**」のインターフェース設定に機器のリストが表示されます。このインターフェースの名前は「名前」列で **U0** または **U1** と表記されます。

3G/4G/LTE 接続種別の設定は、SonicWall 装置で 3G/4G/LTE インターフェースを用いた WAN 接続に対する柔軟な制御を提供します。接続種別は「**接続 | 3G/4G > 接続プロファイル**」でプロファイルを編集する際に設定します。3G/4G プロファイル設定ウィンドウの「**パラメータ**」タブで、以下の接続種別が用意されています。

- **恒久的な接続** - 3G/4G インターフェースが 3G/4G サービス プロバイダに接続されると、管理者が切断するか、ネットワークに関する事象 (WAN が利用可能になる等) によって切断されるまで、接続したままになります。
- **データによる接続** - SonicWall 装置が特定の種別のネットワーク トラフィックを検知した場合に、3G/4G インターフェースが自動的に接続されます。
- **手動接続** - 管理者が手動で接続を開始した場合にのみ、3G/4G インターフェースが接続されます。

△ **注意：3G/4G 接続は、システム セットアップ | ネットワーク > インターフェース ページで (U0/U1 インターフェースの「管理」ボタンを選択することで) 手動で有効にできますが、これにより自動接続が期待通りに機能しなくなる可能性があるため、推奨されません。SonicWall では、上記の接続種別を使って 3G/4G インターフェースを運用することを推奨します。**

SonicWave MiFi Extender

SonicOS 6.5 では、SonicWave 3G/4G/LTE MiFi Extender 機能を使用すると、SonicWall 無線アクセス ポイントを 3G または 4G セルラー ネットワークに接続して無線ホットスポットを作成し、スマートフォン、ノートパソコン、タブレットなどのモバイル機器で共有することができます。この WWAN ソリューションにより、複数のエンド ユーザとモバイル機器が 3G または 4G モバイル ブロードバンド インターネット接続を共有できるようになります。

この機能を使用するには、SonicWave アクセス ポイントに USB 機器を差し込んで、その機器から 3G/4G 経由でインターネットに接続します。SonicOS で、VLAN インターフェースを USB モデムに関連付けます。

この機能は、SonicOS 6.5 を実行するすべての SonicWall ファイアウォールと、USB インターフェースを備えたすべての SonicWave アクセス ポイントでサポートされます。3G、4G、または QMI プロトコルをサポートする USB デバイスが必要です。

VLAN 設定に対して以下の設定を使用します。

- ゾーンを WAN に設定します。
- 親インターフェースを、アクセス ポイントが接続されている物理インターフェースに設定します。
- 3G USB モデムの場合は、ネットワーク モードを静的に設定し、プライベート IP アドレスを割り当てます。ゲートウェイおよび DNS サーバのフィールドは空白のままにします。これらのフィールドは、アクセス ポイントのプロビジョニングが完了すると自動的に設定されます。
- 4G および QMI モデムの場合は、ネットワーク モードを DHCP に設定します。モデムを接続すると USB モデム サーバから DHCP リースが取得されます。

この機能は、MiFi Extender 構成ページで設定された 3G/4G 接続プロファイルの設定を使用します。

3G/4G/LTE フェイルオーバー

重要：プライマリ WAN インターフェースがダウンした場合の 3G/4G/LTE デバイスのフェイルオーバーの動作を管理できます。3G/4G/LTE インターフェースをバックアップ インターフェースとして機能させる場合、既定の負荷分散グループ内の最終バックアップ インターフェースとして設定できます。「**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**」ページに移動して、3G/4G/LTE 機器を含むグループを編集してください。

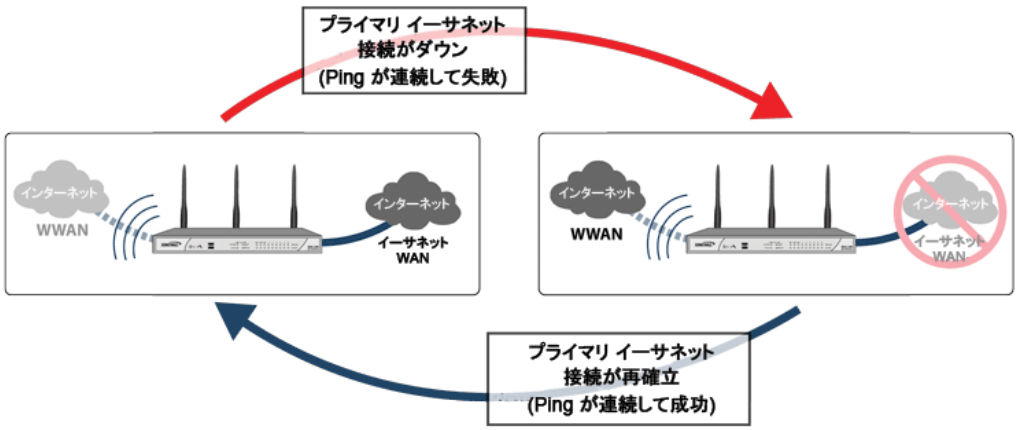
以下のセクションでは、WAN から 3G/4G/LTE へのフェイルオーバーの 3 つの異なる方式について説明します。これらすべてのセクションでは、U0/U1 インターフェースが負荷分散グループ内の最終バックアップ インターフェースとして設定されていることを前提としています。

- 恒久的な接続時の 3G/4G/LTE フェイルオーバー
- 「データによる接続」時の 3G/4G/LTE フェイルオーバー
- 「手動ダイアル」時の 3G/4G/LTE フェイルオーバー

恒久的な接続時の 3G/4G/LTE フェイルオーバー

以下の図は、3G/4G/LTE 接続プロファイルが「**恒久的な接続**」向けに設定されていて WAN イーサネット接続に障害が生じた場合に発生するイベントの順序を示しています。

3G/4G フェイルオーバーのイベント シーケンス: 恒久的な接続



1 **プライマリ イーサネット接続が利用可能な場合** - イーサネット WAN インターフェースが接続され、プライマリ接続として使用されます。イーサネット WAN インターフェースが利用可能である間、U0/U1 インターフェースは接続されません。

2 **プライマリ イーサネット接続が利用できない場合** - U0/U1 インターフェースが始動され、イーサネット WAN 接続がダウンしている間は "*常時接続*" 状態になります。

別のイーサネット WAN インターフェースが負荷分散グループの一部として設定されている場合は、装置は U0/U1 インターフェースにフェイルオーバーする前に、まずセカンダリ イーサネット WAN にフェイルオーバーします。この場合、プライマリおよびセカンダリ WAN がどちらも利用不可能なときにのみ U0/U1 インターフェースへのフェイルオーバーが実行されます。

3 **フェイルオーバー後のプライマリ イーサネット接続の再確立** - イーサネット WAN 接続 (プライマリ WAN ポートまたはセカンダリ WAN ポート、設定されている場合) が復旧すると、すべての LAN-WAN 間トラフィックのルートは利用可能になったイーサネット WAN 接続に自動的に戻ります。これにはアクティブ接続とVPN 接続が含まれます。U0/U1 インターフェース接続が閉じられます。

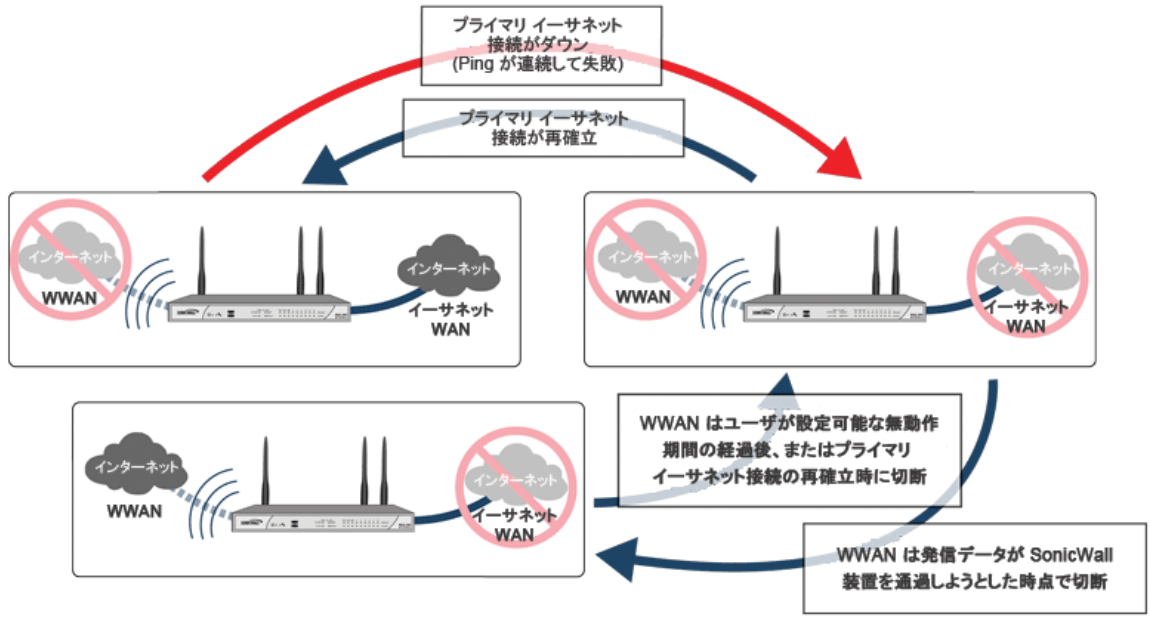
> **メモ：**3G/4G/LTE がバックアップ WAN として設定されている場合は、「**利用可能になった際に、先制して優先インターフェースにフェイルバックする**」チェックボックス (「**システム セットアップ | ネットワーク > 既定の LB グループの編集**」) がオフになっていても、U0 接続はイーサネット WAN が利用可能になったとき切断されます。

> **注意：U0/U1 インターフェースが負荷分散グループの最終バックアップとして設定され稼働している場合は、U0/U1 インターフェースを使用するポリシー ベースのルートは設定しないでください。ポリシーベースのルートが U0/U1 インターフェースを使用するように設定されている場合は、最大接続時間 (設定している場合) に達するまで接続された状態が維持されます。**

「データによる接続」時の 3G/4G/LTE フェイルオーバー

下図は、3G/4G/LTE 接続プロファイルが「**データによる接続**」向けに設定されていて WAN イーサネットの接続に障害が生じた場合に発生するイベントの順序を示しています。

3G/4G フェイルオーバーのイベント シーケンス: データによる接続



1. **プライマリ イーサネット接続が利用可能な場合** - イーサネット WAN インターフェースが接続され、プライマリ接続として使用されます。イーサネット WAN インターフェースが利用可能である場合は、3G/4G/LTE の接続は行われません (送信先インターフェースとして U0/U1 インターフェースが指定されているルートを明示的に設定していない場合)。
2. **プライマリ イーサネット接続を利用できない場合** - 送信データが SonicWall 装置を通過しようとするまでは、U0/U1 インターフェース接続は確立されません。
3. **3G/4G 接続の確立** - 機器またはネットワーク ノードがデータをインターネットに送信しようとすると、U0/U1 インターフェース接続が確立されます。「最大接続時間」 (設定している場合) に達するまで、U0/U1 インターフェースの接続は維持されます。
4. **フェイルオーバー後の WAN イーサネット接続の再確立** - イーサネット WAN 接続が復旧するか無動作タイマー (設定されている場合) の時間に達すると、すべての LAN-WAN 間トラフィックのルートは、利用可能になったイーサネット WAN 接続に自動的に戻ります。U0/U1 インターフェース接続は終了します。

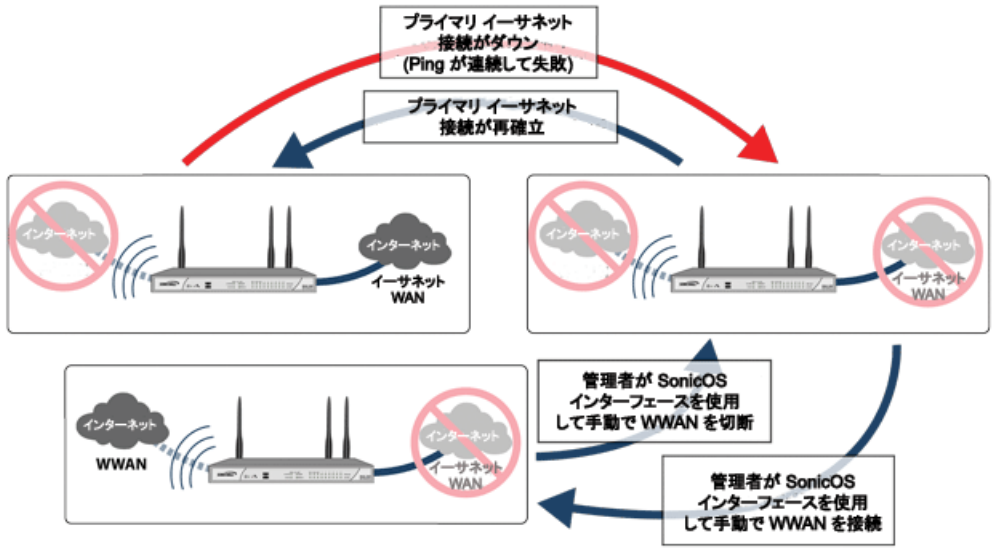
> **メモ：**3G/4G/LTE がバックアップ WAN として設定されている場合は、「**利用可能になった際に、先制して優先インターフェースにフェイルバックする**」チェックボックス (「**システム セットアップ | ネットワーク > 既定の LB グループの編集**」) がオフになっていても、U0 接続はイーサネット WAN が利用可能になったとき切断されます。

> **注意：U0/U1 インターフェースが負荷分散グループの最終バックアップとして設定され稼働している場合は、U0/U1 インターフェースを使用するポリシー ベースのルートは設定しないでください。ポリシーベースのルートが U0/U1 インターフェースを使用するように設定されている場合は、最大接続時間 (設定している場合) に達するまで接続された状態が維持されます。**

「手動ダイアル」時の 3G/4G/LTE フェイルオーバー

> **注意：U0/U1 インターフェースがプライマリ WAN インターフェースのフェイルオーバー バックアップとして使う予定で設定されている場合は、SonicWall では手動でダイアルの 3G/4G 接続プロファイルの使用を推奨していません。WAN の障害発生時に U0/U1 インターフェースが管理者によって手動で開始されるまで、装置が WAN 接続を失った状態になります。下図は、3G/4G 接続プロファイルが手動でダイアル向けに設定されていて WAN イーサネットの接続に障害が生じた場合に発生するイベントの順序を示しています。**

3G/4G フェイルオーバーのイベント シーケンス: 手動でダイアル



1. **プライマリ イーサネット接続が利用可能な場合** - イーサネット WAN インターフェースが接続され、プライマリ接続として使用されます。イーサネット WAN 接続が利用可能である場合は、3G/4G/LTE の接続は行われません。
2. **プライマリ イーサネット接続を利用できない場合** - 管理者が接続を手動で有効にするまで、U0/U1 インターフェース接続は確立されません。
3. **3G/4G 接続の確立** - 管理者が SonicWall 装置で U0/U1 インターフェース接続を手動で有効にすると、接続が確立されます。手動で接続を無効にするまで、U0/U1 インターフェースの接続は維持されます。
4. **フェイルオーバー後の WAN イーサネット接続の再確立** - イーサネット接続が復旧したかどうかにかかわらず、接続を手動で無効にするまで、**すべての LAN-WAN 間トラフィックには手動で有効にした 3G/4G 接続**が引き続き使用されます。手動で切断すると、利用可能なイーサネット接続が使用されます。

3G/4G/LTE の前提条件

3G/4G/LTE インターフェースを設定する前に、次の前提条件を満たす必要があります。

- サポートされているサードパーティ無線プロバイダから 3G/4G/LTE サービス プランを購入する
- 3G/4G/LTE デバイスを設定してアクティブ化する
- SonicWall セキュリティ装置の電源を入れる**前**に、3G/4G/LTE デバイスを SonicWall 装置に挿入する

  重要：3G/4G/LTE デバイスの抜き差しは、必ず SonicWall セキュリティ装置の電源が入っていない状態で行います。

U0/U1 インターフェースを有効にする

3G/4G/LTE USB モデムが SonicWall セキュリティ装置に接続されている場合、SonicOS はそのモデルを検知し、「**管理 | システム セットアップ | ネットワーク > インターフェース**」ページで 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、フェイルオーバーと負荷分散に使用できます。U0 構成設定には、デバイス種別、「データによる接続」の種別、および管理/ユーザ ログインのオプションが含まれています。U0 インターフェースには、接続マネージャにアクセスするための「**管理**」ボタンもあります。

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します。接続が確立される前、U0 の接続マネージャの状況は *切断*です。

メモ：すべての 3G/4G/LTE USB デバイスでは、「**接続**」ボタンを選択する前に 3G/4G プロファイルを作成する必要があります。

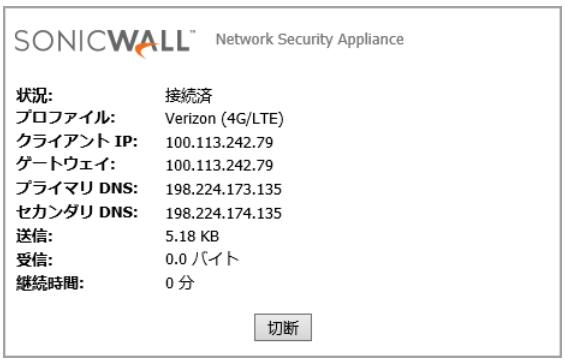
注意：3G/4G/LTE 接続を「ネットワーク > インターフェース」ページで (U0/U1 インターフェースの「管理」ボタンを選択して) 手動により繰り返し有効にすることは推奨されません。これにより自動接続が期待通りに機能しなくなる可能性があります。SonicWall では、3G/4G/LTE 接続種別で説明している接続種別を使って 3G/4G/LTE インターフェースを運用することを推奨します。

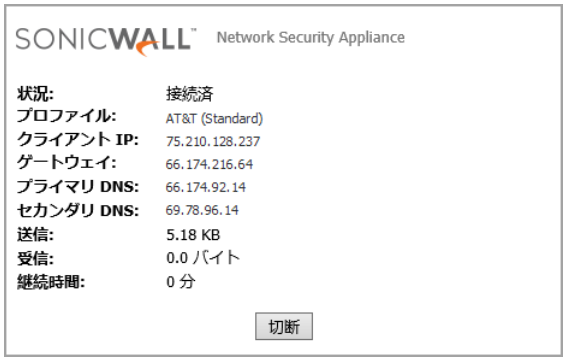
U0/U1 外部 3G/4G/LTE インターフェースで接続を手動により開始するには:

1 「**ネットワーク > インターフェース**」ページで、U0/U1 インターフェースの「**管理**」ボタンを選択します。「**U0/U1 接続状況**」ダイアログが表示されます。

2 「**接続**」ボタンを選択します。WAN インターフェース 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。SonicOS は、この DHCP IP アドレスを U0 インターフェース IP アドレスに使用します。

接続がアクティブになると、「**U0/U1 接続状況**」 (接続マネージャ) にセッションの統計が表示されます。4G/LTE デバイスと 3G (PPP) デバイスの画像を以下に示します。





メモ：DNS サーバ アドレス 192.168.1.1 は一時的な IP アドレスです。このアドレスは、既定の内部 DNS サーバ アドレスです。このアドレスは IP アドレスの競合を引き起こす可能性があるため、SonicOS で DNS サーバ アドレスとして使用することはできません。ATT Velocity / Huawei E3372 LTE デバイスの場合、デバイスは実際の DNS サーバ情報を取得するための AT コマンド インターフェースを提供しません。ただし、LTE モデムの内部ウェブ サーバには有効な DNS サーバがあります。HTTP 通信チャンネルは SonicOS によって開始され、この有効な DNS サーバ アドレスを取得します。

3 接続を終了するには、「**切断**」をクリックします。

36

3G/4G/モデム基本設定の設定

3G/4G/LTE 機器またはモデムを設定する最初のステップは、基本設定の定義です。「3G/4G/モデム概要」でも注記されているように、装置は接続されている機器の種別を検知しようとします。種別を特定することに成功した場合、検知されたものが左側のナビゲーションおよび設定ページに代わりに表示されます。機器を手動で選択する場合は、「デバイスの検知とインターフェースの選択」を参照してください。

以下の基本設定を定義する必要があります。

3G/4G/LTE 機器に対して	モデムに対して
3G/4G/LTE 設定	モデムの設定
データ種別による接続	データ種別による接続
管理/ユーザ ログイン	管理/ユーザ ログイン

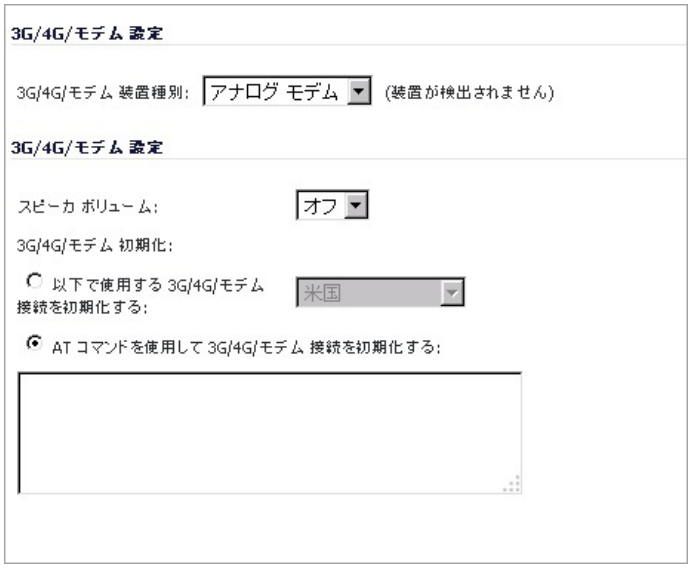
トピック:

- 設定
- データ種別による接続
- 管理/ユーザ ログイン
- MiFi Extender の設定

設定

このセクションで提供されている指示に対して、機器は装置から自動検知されるか、手動で設定されるかのどちらかです。次の画像は、3G/4G/LTE 機器種別が自動検知された例を示しています。

これは、モデムに対しても同じオプションを示します。2 つのモデム設定セクションがあることに注意してください。1 つ目はモデムが自動検知された場合です。2 つ目は設定する必要があるオプションがある場合です。

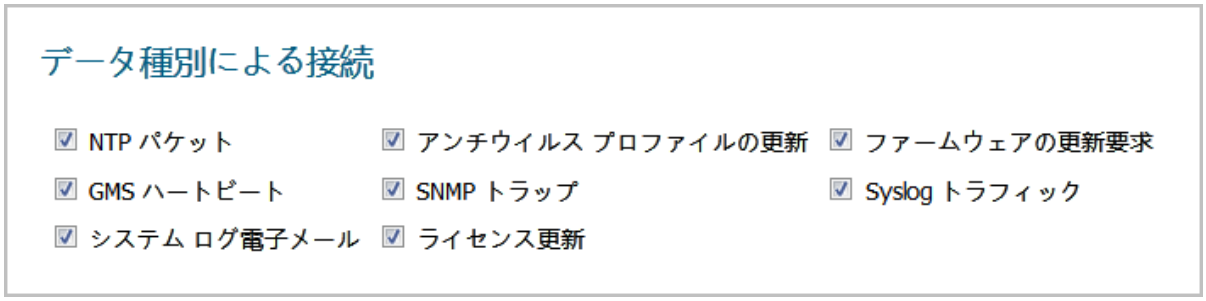


モデム インターフェースを介した SonicWall 装置の管理を有効にするには、「**モデム設定**」セクションで設定を行う必要があります。

- **スピーカ ボリューム** - スピーカの「**オン**」または「**オフ**」 (既定) を選択します。
- 「**3G/4G モデム初期化**」- 次のいずれかのオプションを選択します。
  - **以下で使用する 3G/4G モデム接続を初期化する** - ドロップダウン リストから国を選択します。
  - **AT コマンドを使用して 3G/4G モデム接続を初期化する** - 適切な AT コマンドをフィールドに入力します。

データ種別による接続

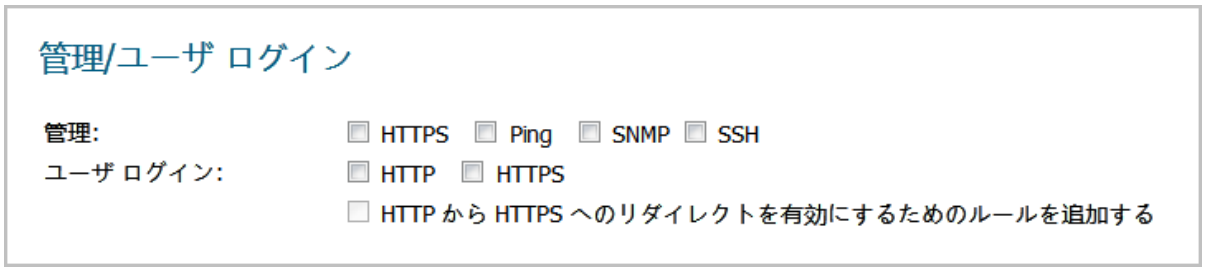
機器種別として「**3G/4G/LTE/モバイル**」または「**アナログ モデム**」を選択した場合は、「**データ種別による接続**」セクションが表示されます。このセクションでは、SonicWall 装置が特定の種別のトラフィックを検出した際に、インターフェースがサービス プロバイダに自動的に接続するように設定できます。「**データ種別による接続**」は、既定ですべて選択されています。



「デー種別タによる接続」を実施するように SonicWall 装置を設定するには、接続プロファイルの「**接続種別**」として「**データ種別による接続**」を選択する必要があります。詳細については、「3G/4G/モデムの接続プロファイルの設定」を参照してください。

管理/ユーザ ログイン

機器種別として「**3G/4G/LTE/モバイル**」または「**アナログ モデム**」を選択した場合は、「**管理/ユーザ ログイン**」セクションが表示されます。インターフェースを介した SonicWall 装置のリモート管理を有効にするには、「**管理/ユーザ ログイン**」セクションで設定を行う必要があります。



「**管理**」フィールドでは、サポートされているプロトコルのいずれかまたはすべてを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** の中から 1 つ以上の管理オプションを選択します。

メモ：ISP によっては、ISP が提供する IP アドレスでの HTTPS または Ping 管理を許可していません。

「**ユーザ ログイン**」フィールドでは、「**HTTP**」か「**HTTPS**」か両方かを「**選択**」してください。HTTP トラフィックは HTTPS トラフィックよりも安全性が低いことに注意してください。

「**管理**」や「**ユーザ ログイン**」で HTTPS を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」オプションが自動的に選択されます。このオプションを有効にすると、ファイアウォールは HTTP 要求を自動的に HTTPS 要求に変換してセキュリティを強化します。変換したくない場合は、このオプションをオフにします。

メモ：以前の SonicOS リリースでは、「**3G/4G > 設定**」ページ上で 3G/4G インターフェースのプローブ監視を設定していました。現在は、プローブ監視は「**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**」で設定します。詳細については、*SonicOS 6.5 システム設定*を参照してください。

MiFi Extender の設定

3G/4G/LTE MiFi Extender 機能を使用すると、SonicWall SonicWave アクセス ポイントを 3G または 4G セルラー ネットワークに接続して無線ホットスポットを作成することができます。複数のエンド ユーザとモバイル機器が 3G または 4G モバイル ブロードバンド インターネット接続を共有できます。

この機能を使用するには、SonicWave アクセス ポイントに USB 機器を差し込みます。SonicOS で、VLAN インターフェースを USB モデムに関連付けます。

アクセス ポイントを設定するには、以下の手順に従います。

1. 「**管理**」ビューで、「**接続性 | アクセス ポイント > 基本設定**」に移動します。
2. 「**SonicPoint / SonicWave オブジェクト**」で、使用するアクセス ポイントの「**設定**」ボタンを選択します。
3. 「**3G/4G/LTE WWAN**」ボタンを選択します。

メモ：このページの下部にある「**3G/4G/LTE WWAN ウィザード**」ボタンを選択すると、ウィザードの指示に従って VLAN インターフェースと 3G/4G/LTE 接続プロファイルを作成または選択することができます。

4 「**3G/4G/LTE モデムを有効にする**」チェックボックスをオンにします。

5 USB 機器用に作成した VLAN を「**WAN VLAN インターフェースへの関連付け**」ドロップダウン リストから選択します。

6 特定の接続プロファイルを使用するには、「**接続プロファイルを有効にする**」チェックボックスをオンにして、関連するフィールドに入力します。多くの場合は、既定の接続プロファイルを使用できます。その場合、この手順は省略可能です。

7 「**OK**」を選択します。

設定がアクセス ポイントに適用されます。基本的な状況は「**管理**」ビューの「**接続性 | アクセス ポイント > 3G/4G/LTE WWAN**」ページで確認できます。

複数のアクセス ポイントと 3G/4G モデム (それぞれ最低 2 台) が利用可能な場合、SonicOS はそれらを同時に利用して負荷分散を実行できます。まず、SonicPoint とモデムの各ペアに一意の VLAN を割り当てます。次に、「**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**」ページでそれらの VLAN インターフェースを負荷分散グループに追加します。

37

3G/4G/モデム詳細設定の構成

「**詳細設定**」ページでは、3G/4G/LTE 機器およびモデムについて、次の機能を設定します。

- ダイアル アウトの遠隔開始設定
- 帯域幅管理
- 接続の制限

ダイアル アウトの遠隔開始設定

「**ダイアル アウトの遠隔開始**」セクションでは、リモートから WAN モデム接続を開始できます。以下の手順では、ダイアル アウトの遠隔開始の呼び出し方法について説明します。

1 ネットワーク管理者が、リモート オフィスにある SonicWall セキュリティ装置へのモデム接続を開始します。

2 装置が着信コールを認証するように設定してある場合は、ネットワーク管理者にパスワードの入力を要求します。コールが認証されると、装置はそのコールを終了します。

3 その後で、装置は設定されたダイアル プロファイルに基づいて、ダイアルアップ ISP へのモデム接続を開始します。

4 装置のウェブ管理インターフェースにアクセスして、必要なタスクを実行します。

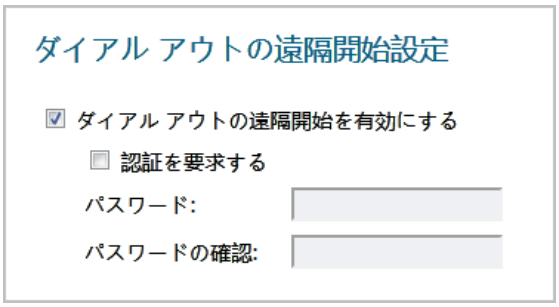
ダイアル アウトの遠隔開始機能を設定する前に、設定内容が次の前提条件を満たしているかどうかを確認してください。

- 3G/4G 接続プロファイルが「**ダイアルオン データ**」に設定されていること。
- SonicWall セキュリティ装置が、**HTTPS** を使用して管理される設定になっていること (この設定の場合、機器へのリモート アクセスが可能)。
- 必須ではありませんが、「**無動作時に切断を有効化**」には数値を入れておくことをお勧めします。このフィールドは、「**プロファイルの設定**」「**>**」「**パラメータ**」ページにあります。機器に対するプロファイルを編集してアクセスします。このフィールドに値を入力しないと、ダイアル アウトの呼び出しが無期限に接続された状態になるため、「**切断**」ボタンを選択して手動でセッションを終了しなければならなくなります。

ダイアル アウトの遠隔開始を設定するには:

1 「**管理**」表示で、「**詳細**」ページに移動します。

- **接続 | 3G/4G > 詳細設定**
- **接続 | モデム > 詳細設定**



2 「**ダイアル アウトの遠隔開始を有効にする**」チェックボックスをオンにします。

3 リモート接続に対して認証を必須にしたい場合には、「**認証を要求する**」チェックボックスをオンにして、「**パスワード**」と「**パスワードの確認**」フィールドにパスワードを入力してください。

4 「**適用**」を選択して変更を保存します。

帯域幅管理

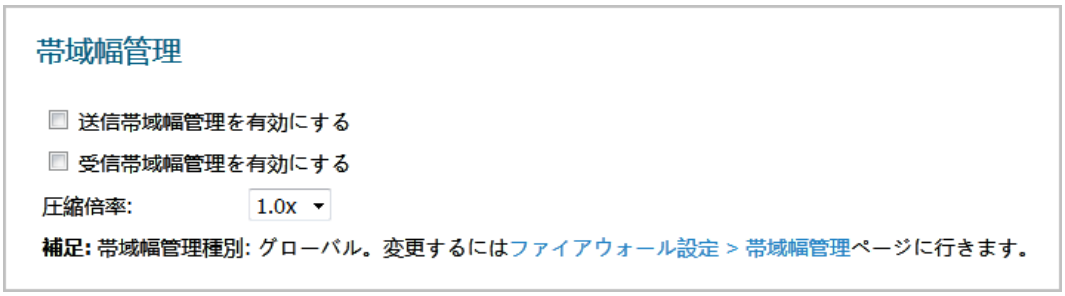
「**帯域幅管理**」セクションでは、3G/4G インターフェースの送信または受信帯域幅管理サービスを有効にできます。

メモ：帯域幅管理の設定についての情報は、「*SonicOS 6.5 セキュリティ設定*」の**ファイアウォール設定**を参照してください。

帯域幅管理を設定するには:

1 「**管理**」表示で、「**詳細**」ページに移動します。

- **接続 | 3G/4G > 詳細設定**
- **接続 | モデム > 詳細設定**



2 **送信帯域幅管理を有効にする**には、該当するチェック ボックスをオンにします。

3 **受信帯域幅管理を有効にする**には、該当するチェック ボックスをオンにします。

4 「**圧縮倍率**」をドロップダウン メニューで以下の中から選択します。

1.0x (既定)、**1.5x**、**2.0x**、**2.5x**、**3.0x**、**3.5x**、**4.0x**

圧縮倍率は、送信と受信の両方の帯域幅に適用されます。

5 「**適用**」を選択して変更を保存します。

帯域幅管理の下にある注では、どの帯域幅管理が選択されたかが表示され、必要があれば変更できるようリンクが提供されます。

接続の制限

「**接続の制限**」セクションでは、3G/4G またはモデム接続にホスト/ノードの制限を設定できます。この機能は、特に、オーバーフローとしてモデム接続を使用している配備や負荷分散状況にある配備において、接続の超過を回避するのに役立ちます。

「**最大ホスト数**」フィールドに、このインターフェースが接続されたときに許可されるホストの最大数を入力します。既定値は "**0**" で、この場合はノード数の制限はありません。

38

3G/4G/モデムの接続プロファイルの設定

「**接続プロファイル**」ページでは、3G/4G/LTE およびモデム接続プロファイルを設定できます。プライマリ プロファイルおよびバックアップ プロファイルも設定できます。

トピック:

プロファイルの設定

時刻を設定するには、以下の手順に従います。

1 「**管理**」表示で、「**接続プロファイル**」ページに移動します。

- **接続 | 3G/4G > 接続プロファイル**
- **接続 | モデム > 接続プロファイル**

2 「**プロファイルの設定**」セクションで、「**プライマリプロファイル**」ドロップダウン メニューから接続プロファイルを選択します。

> **メモ**：モデムに対するオプションは、3G/4G/LTE 機器に対して一覧表示されるものと異なります。

3 必要があれば、「**バックアップ プロファイル 1**」および「**バックアップ プロファイル 2**」もドロップダウン メニューから選択します。

4 「**適用**」を選択して変更を保存します。

接続プロファイル

接続プロファイルを作成するために「**追加**」ボタンを押すか、既存のものを編集するためにテーブルの「**設定**」列で**編集**アイコンをクリックします。

以下のセクションの手順を実行します。

モデムに対して	3G/4G 機器に対して	LTE 機器に対して
一般設定	一般設定	一般設定
ISP アドレス		
パラメータ設定	パラメータ設定	パラメータ設定
	IP アドレス設定	IP アドレス設定
スケジュール設定	スケジュール設定	スケジュール設定
	データ制限	データ制限
詳細	詳細	

メモ：「**基本設定**」ページで選択した「**3G/4G/モデム機器種別**」によっては、表示されないオプションもあります。

一般設定

接続プロファイルを追加または更新した場合、最初の画面では「**一般設定**」が表示されてサービスプロバイダを設定します。「国」、「サービス プロバイダ」、および「プラン種別」を選択すると、多くのサービス プロバイダについては残りのフィールドが自動的に設定されます。

一般的な接続設定を行うには

PPP モデム設定

LTE モデムの設定

1 SonicWall 装置が配備されている「**国**」を選択します。

2 アカウントを作成した「**サービス プロバイダ**」を選択します。

メモ：選択した国でサポートされているサービス プロバイダのみ表示されます。

3 「**プラン種別**」ドロップダウン メニューから、サービス プロバイダに申し込んだプランを選択します。指定の「プラン種別」に応じて、以下の手順に従います。

- 指定のプラン種別がドロップダウン メニューに表示されている場合は (基本プランの多くは、単に「**標準**」と表示されます)、「**一般**」タブの残りのフィールドは自動的に設定されます。これらのフィールドが適切かどうかを確認してから「パラメータ設定」にスキップします。
- 指定の「プラン種別」がドロップダウン メニューに表示されていない場合は、「**その他**」を選択します。

4 「**プロファイル名**」フィールドにプロファイルの名前を入力します。

5 LTE モデムの場合、「**優先ネットワーク技術**」を選択します。以下から選択します。

- **グローバル**
- **LTE/CDMA**
- **GSM/UMTS**

6 LTE モデムの場合、**APN** 値を入力します。

7 PPP モデムの場合、適切な「**接続種別**」が選択されていることを確認します。

メモ：ほとんどのサービス プロバイダについては、このフィールドが自動的に設定されます。

8 PPP モデムの場合、「**ダイアル番号**」が正しいことを確認します。

メモ：ほとんどのサービス プロバイダに対し、ダイアル番号は「***99#**」になります。

9 PPP モデムの場合、プロバイダで必要とされていれば、「**ユーザ名**」、「**ユーザ パスワード**」および「**ユーザ パスワードの確認**」フィールドにそれぞれユーザ名とパスワードを入力します。

ISP アドレス

ISP アドレス設定は、モデムに対してのみ表示されます。これは、モデムがインフラ全体とどのように通信するかを定義するものです。

ISP アドレスを設定するには、以下の手順に従います。

1 「**ISP アドレス**」を選択します。

2 「**IP アドレス**」で、次のいずれかを選択します。

- **自動的に IP アドレスを取得する**
- **IP アドレスを指定する**。アドレスをフィールドに入力します。

3 「**DNS サーバ**」では、次のいずれかを選択します。

- **自動的に IP アドレスを取得する**
- **IP アドレスを指定する**。プライマリ DNS サーバアドレスを最初のフィールドに、セカンダリ DNS サーバアドレスを次のフィールドに入力します。

パラメータ設定

「**パラメータ**」設定では、サービスを接続する条件を設定できます。接続種別には、「恒久的な接続」、「**データによる接続**」、「**手動接続**」の 3 種類があります。これらの接続種別の仕組みについては、「3G/4G/LTE について」を参照してください。

パラメータ設定を構築するには、以下の手順に従います。

1 「**パラメータ**」を選択する。

2 「**接続種別**」ドロップダウン メニューで、接続プロファイルとして「**恒久的な接続**」、「**データによる接続**」、または「**手動接続**」を選択します。

メモ：SonicWall 装置にダイアル アウトの遠隔開始を設定するには、「**接続種別**」を「**データによる接続**」に設定する必要があります。

3 「**無動作時に切断 (分)**」のチェックボックスをオンにして、無動作が継続した際に接続を切断するまでの時間を分で入力します。「**接続種別**」が「**恒久的な接続**」の場合、このオプションは利用できません。

4 「**最大接続時間 (分)**」のチェックボックスをオンにして、動作中か無動作かを問わず、接続を継続する時間を分で入力します。

5 「**再接続前の間隔 (分)**」に値を入力し、指定の時間 (分) が経過すると SonicWall 装置が自動的に再接続するようにします。

6 「**電話番号ごとの再試行回数**」チェックボックスをオンにし、フィールドに数値を入力して、SonicWall 装置が再接続を試行する回数を指定します。

7 「**再試行間隔 (秒)** 」チェックボックスをオンにし、フィールドに値を入力して再試行の間隔 (秒) を指定します。

8 「**ダイアル時に VPN を無効にする**」チェックボックスをオンにし、3G/4G インターフェースを介した VPN 接続を無効にします。

9 「**PAP 認証を強制する**」チェックボックスをオンにします。

IP アドレス設定

「**IP アドレス設定**」を使用して、3G/4G/LTE インターフェースに動的 IP を使用するか静的 IP を使用するかを設定します。ほとんどの場合、この機能は「**自動的に IP アドレスを取得する**」に設定されていますが、利用するサービス プロバイダで必要な場合は、ゲートウェイ IP アドレスおよび 1 つ以上の DNS サーバ IP アドレスの両方について手動で IP アドレスを設定できます。

IP アドレスを設定するには:

1 「**IP アドレス**」を選択します。

既定では、3G/4G 接続プロファイルには IP アドレスと DNS サーバ アドレスを自動的に取得するよう設定されています。

2 静的な IP アドレスを指定するには、「**IP アドレスを指定する**」ラジオ ボックスをオンにし、フィールドに IP アドレスを入力します。

3 DNS サーバ アドレスを手動で入力するには、「**IP アドレスを指定する**」ラジオ ボックスをオンにし、プライマリおよびセカンダリ DNS サーバの IP アドレスをフィールドに入力します。

スケジュール設定

「**スケジュール**」を使用すると、特定の曜日の特定の時間に接続を限定できます。この機能は、夜間または週末に非稼働時間があるプランなど、時間によるアクセス制限が設定されているデータ プランを利用するときに便利です。

メモ：この機能を有効にした場合、曜日のチェックボックスが**オフ**になっていると、その曜日の 3G/4G/LTE アクセスは終日拒否されます。

アクセス スケジュールを設定するには:

1 「**スケジュール**」を選択します。

2 「**接続プロファイルの制限時間**」チェックボックスをオンにして、このインターフェースのスケジュール機能を有効にします。

3 アクセスを許可する**曜日**のチェックボックスをオンにします。

4 各曜日の**開始時間**および**終了時間**を 24 時間形式で入力します。

データ制限

「**データ制限**」は、3G/4G/LTE 機器でのみ利用可能です。月単位でデータ使用量を制限できます。この機能により、3G/4G/LTE プロバイダの課金サイクルに応じて使用量を追跡し、指定した制限に達したときに切断することができます。

データ使用量を制限するには:

1 「**データ制限**」をクリックします。

ヒント：3G/4G/LTE アカウントに月ごとのデータ制限または時間制限がある場合は、データ使用制限を有効にすることを強くお勧めします。

2 「**データ使用制限を有効にする**」チェックボックスをオンにして、その月のデータや時間の指定制限に達すると 3G/4G/LTE インターフェースが自動的に停止するようにします。

3 「**課金サイクルの開始日**」ドロップダウン メニューから、データまたは時間の使用量の追跡を開始する日付を選択します。

4 「**制限**」フィールドに値を入力し、制限を適用する単位を、「**GB**」、「**MB**」、「**KB**」、「**分**」から選択します。

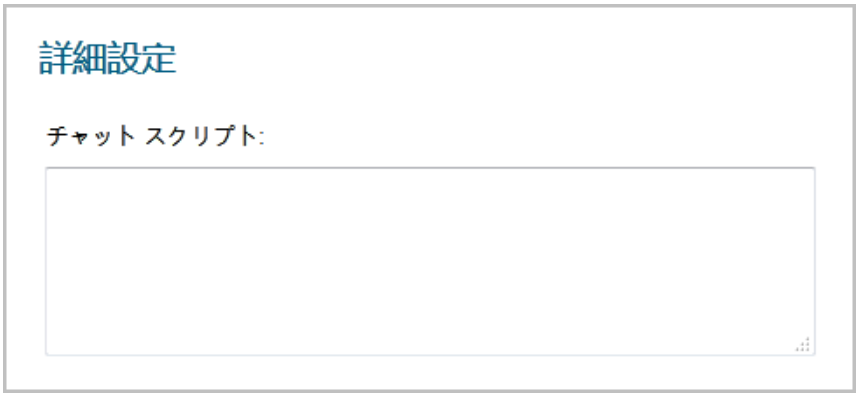
詳細

「**詳細**」タブでは、3G/4G 接続プロセス時に使われるチャット スクリプトを手動で設定できます。

ヒント：チャット スクリプトは、標準のダイアルアップ接続スクリプトにコマンドや特別な命令を追加する必要がある場合にのみ設定します。

チャット スクリプトを設定するには:

1 「**詳細**」タブを選択します。



2 「**チャット スクリプト**」フィールドに接続チャット スクリプトを入力します。

3 「**OK**」を選択します。

39

3G/4G データ転送の監視

「**管理**」表示の「**接続 | 3G/4G > データ使用**」に移動して、「**データ使用**」監視と「**セッション履歴**」表示を行います。

「**データ使用**」テーブルには、現在の「**年**」、「**月**」、「**週**」、「**日**」と、「**集計周期**」ごとに現在のデータ使用量とオンライン時間が表示されます。集計周期における使用量は、3G/4G 接続プロファイルの「**データ使用制限を有効にする**」オプションが有効な場合にのみ計算されます。

いずれかの種別のデータ使用量をリセットするには、対応する「**リセット**」ボタンを選択します。

メモ：「**データ使用**」テーブルには現在の使用量の概算だけが表示されます。実際の課金の計算に使用することはできません。正確な課金情報については、サービス プロバイダにお問い合わせください。

「**セッション履歴**」テーブルには、3G/4G/LTE セッションに関する情報の概要が表示されます。特定のセッションの詳細を確認するには、「**プロパティ**」列の**コメント** アイコン上にマウス カーソルを合わせます。テーブルをクリアするには、「**クリア**」ボタンを選択します。

第 6 部

接続性 | 付録

- 仮想アクセス ポイントの設定例
- SonicWall サポート

40

仮想アクセス ポイントの設定例

このセクションでは、現実の無線ニーズに基づいた仮想アクセス ポイントの設定例を示します。

トピック:

- 学校職員のアクセス用 VAP の設定
- ワイヤレス無線機への VAP の配備

学校職員のアクセス用 VAP の設定

一般的にオフィスやキャンパスにいるユーザの集まりに対し、すべてのネットワーク リソースへの完全なアクセスを認めるべきである場合に、接続が認証されて安全であるならば、VAP を使用することができます。これらのユーザはすでにネットワークのディレクトリ サービスである Microsoft アクティブ ディレクトリに属しています。これはインターネット認証サービス (IAS) を通じて EAP インターフェースを提供します。このセクションには次の内容が含まれています。

- ゾーンの設定
- 新規無線サブネットの作成
- 無線 VAP プロファイルの作成
- 無線 VAP の作成
- さらに作成 > 現在の VAP を使用

ゾーンの設定

このセクションでは、SonicWall ファイアウォールセキュリティサービスと、強化された WiFiSec/WPA2 無線セキュリティを備えた、新しい社内無線ゾーンを作成して設定します。ゾーンに関する詳細については、*SonicOS 6.5 システム設定* を参照してください。

1 SonicWall ネットワーク セキュリティ装置の管理インターフェースにログインします。

2 「**管理**」表示を選択します。

3 「**システム セットアップ**」で「**ネットワーク > ゾーン**」を選択します。

4 「**追加...**」ボタンを選択して、新しいゾーンを追加します。

「一般設定」タブ

1 「**一般設定**」タブで、「**名前**」フィールドに "WLAN_Faculty" などのニックネームを入力します。

2 「**セキュリティ種別**」ドロップダウン メニューで「**無線**」を選択します。

3 「**インターフェース間通信を許可する**」チェックボックスをオンにして、職員ユーザ間の通信を許可します。

4 無線 LAN で接続する職員に通常適用するセキュリティサービスのチェックボックスをすべてオンにします。

「無線の設定」タブ

1 「**SonicPoint/SonicWaveにより生成された通信のみ許可する**」チェックボックスをオンにします。

2 「**SonicPoint プロビジョニング プロファイル**」ドロップダウン メニューからプロファイルを選択します (該当する場合)。

3 「**OK**」ボタンを選択して、変更内容を保存します。

これで新しいゾーンが「**ネットワーク > ゾーン**」ページの下部に表示されるようになります。ただし、まだメンバー インターフェースにリンクされていません。これは次の手順で行います。

新規無線サブネットの作成

このセクションでは、現在の WLAN 上に新しい無線サブネットを作成して設定します。この無線サブネットは、以前に「ゾーンの設定」で作成したゾーンにリンクされます。

新規無線サブネットを作成するには、以下の手順に従います。

1 「**管理**」画面において、「**システム セットアップ| ネットワーク >インターフェース**」ページを選択します。

2 「**インターフェースの追加**」フィールドで「**仮想インターフェース**」を選択します。

3 「**ゾーン**」ドロップダウンメニューで、以前に作成したゾーンを選択します。この例では、**WLAN_Faculty** を選択します。

4 このインターフェースの **VLAN タグ**を入力します。VLANによって、このサブネットに属するトラフィックを内部ワイヤレス無線機が識別できます。この例では、サブネットVLANのタグとして100を選択します。

5 「**親インターフェース**」から「**W0**」を選択します。

6 このサブインターフェースの「**IP アドレス**」を入力します。

7 「**OK**」ボタンを選択して、このサブインターフェースを追加します。

これで WLAN サブネット インターフェースが「インターフェース設定」リストに表示されるようになります。

無線 VAP プロファイルの作成

このセクションでは、新しい仮想アクセスポイントプロファイル (VAP) を作成して設定します。VAP の種別ごとに VAP プロファイルを作成し、それらを使って新しい VAP に詳細設定を簡単に適用することができます。このセクションの内容は任意設定項目ですが、これによって複数の VAP の設定がずっと簡単になります。

無線 VAP プロファイルを作成するには、以下の手順に従います。

1 「**管理**」表示を選択します。

2 「**接続**」で「**無線 > 仮想アクセス ポイント**」を選択します。

3 「**仮想アクセス ポイント プロファイル**」セクションの「**追加**」ボタンをクリックします。

4 ドロップダウンリストから「**VAP スケジュール名**」を選択します。

5 この VAP プロファイルの**プロファイル名**を入力します ("Corporate-WPA2" など)。

6 「**認証種別**」ドロップダウン メニューから「**WPA2-自動-EAP**」を選択します。これにより、現在の RADIUS サーバ設定 (後ほど設定) に基づいて自動ユーザ認証が使用されます。

7 「**最大クライアント数**」フィールドに、VAP でサポートする必要がある同時接続の最大数を入力します。

8 「**RADIUS サーバの設定**」セクションで、現在の RADIUS サーバの情報を入力します。この情報は、新しいサブネットへの認証されたログインをサポートするために使われます。

9 「**OK**」ボタンを選択して、この VAP プロファイルを作成します。

無線 VAP の作成

このセクションでは、新しい仮想アクセス ポイント (VAP) を作成して設定し、「新規無線サブネットの作成」で作成した無線サブネットと関連付けます。

無線 VAP を作成するには、以下の手順に従います。

一般

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

2 「**仮想アクセス ポイント**」セクションの「**追加**」ボタンを選択します。

3 「**名前**」フィールドに、わかりやすい名前を入力します。

4 VAP の **SSID** 名を入力します。この例では、"**Campus_Faculty**" にします。接続する無線ネットワークをユーザが選択するときには、この名前が表示されます。

5 ドロップダウンリストから「**VLAN ID**」を選択します。作成したものがリスト内に表示されているはずです。この例では、「WLAN_Faculty」サブネットの VLAN タグを選択します。

6 「**仮想アクセス ポイントを有効にする**」チェックボックスをオンにします。

7 この SSID をユーザから隠すには、「**SSID抑制を有効にする**」チェックボックスをオンにします。

8 「**OK**」ボタンを選択して、この VAP を追加します。

これで新しい VAP が「仮想アクセス ポイント」リストに表示されるようになります。

詳細

1 「**詳細設定**」を選択して、暗号化設定を編集します。

2 前のセクションで VAP プロファイルを作成した場合は、そのプロファイルを「**プロファイル名**」ドロップダウン メニューから選択します。「Corporate-WPA2」プロファイルを作成して選択します。このプロファイルでは、認証方式として **WPA2-自動-EAP** を使用します。VAP プロファイルをセットアップしていない場合は、手順 2〜4 を実行してください。セットアップしている場合は、「さらに作成 > 現在の VAP を使用」に進んでください。

3 「**詳細設定**」タブで、「**認証種別**」ドロップダウン メニューから「**WPA2-自動-EAP**」を選択します。これにより、現在の RADIUS サーバ設定 (後ほど設定) に基づいて自動ユーザ認証が使用されます。

4 「**最大クライアント数**」フィールドに、VAP でサポートする同時接続の最大数を入力します。

5 「**WPA-EAP 暗号化の設定**」セクションで、現在の RADIUS サーバの情報を入力します。この情報は無線サブネットへの認証されたログインをサポートするために使われます。

さらに作成 > 現在の VAP を使用

以上で職員のアクセス用の無線サブネットのセットアップが完了したので、この後は個別 VAP をさらに追加することもできますし、この設定を内部ワイヤレス無線機に配備することもできます。

ヒント：VAP は後でいつでも追加することができます。追加した VAP は、「ワイヤレス無線機への VAP の配備」の手順に従って、同時に配備することができます。

ワイヤレス無線機への VAP の配備

次のセクションでは、新しい VAP をグループ化して配備し、内部ワイヤレス無線機と関連付けます。このプロセスが完了するまで、ユーザは VAP にアクセスできません。

- 複数の VAP のグループ化
- VAP グループとワイヤレス無線機との関連付け

複数の VAP のグループ化

このセクションでは、複数の VAP をグループ化して 1 つにまとめます。このグループは後で物理的アクセスポイントと関連付けます。

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

2 **内部APグループ**の「**編集**」ボタンをクリックします。

3 リストから目的の VAP を選択し、-> ボタンを選択して、それらの VAP をグループに追加します。オプションで「**すべて追加**」ボタンを選択して、すべての VAP を単一のグループに追加します。

4 「**OK**」ボタンを選択して、変更内容を保存すると共にグループを作成します。

5 802.11g WEP または 802.11a WEP/WPA 暗号化を設定する、もしくは MAC アドレスフィルタリングを有効化するには、仮想アクセスポイントまたは仮想アクセスポイントプロファイルを編集して、「**詳細設定**」タブに移動します。いずれかの VAP で暗号化を使用する場合、無線 VAP を機能させるためには、これらの設定を行う必要があります。

6 「**OK**」ボタンを選択して、変更内容を保存すると共に、この無線プロビジョニング プロファイルを作成します。

VAP グループとワイヤレス無線機との関連付け

VAP を設定して**内部 AP グループ**に追加した後で、内部ワイヤレス無線機を通じてそれらの VAP を使用可能にするために、「**無線 > 設定**」ページでそのグループを指定する必要があります。

1 「**接続 | 無線 > 基本設定**」ページに移動します。

2 「無線仮想アクセス ポイント」セクションの「**無線仮想アクセス ポイント グループ**」ドロップダウンメニューから、「**内部 AP グループ**」を選択します。

3 「**承諾**」ボタンを選択して続行し、この VAP グループを内部ワイヤレス無線機に関連付けます。

メモ：ゲスト サービスを初めてセットアップする場合は、「**ユーザ > ゲスト サービス**」の *SonicOS 6.5 システム設定* にある説明に従って、必要な設定を必ず行ってください。

41

SonicWall 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。

このドキュメントについて

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おそ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。

SonicOS 6.5 接続 管理
更新日 - 2019 年 9 月
ソフトウェア バージョン - 6.5.4
232-002571-04 Rev A

エンド ユーザ製品契約

SonicWall エンド ユーザ製品利用規約を参照する場合は、https://www.sonicwall.com/ja-jp/legal/license-agreements に移動してください。

オープン ソース コード

SonicWall では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、"SonicWall Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035