SonicOS および SonicOSX 7 IPSec VPN

管理ガイド

SONICWALL®

目次

1

IPSec VPN の概要

補足: SonicOS/X という表記は、その機能が両方の SonicOS および SonicOSX で使用可能なことを示します。

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 トンネル インターフェース 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
- 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、および「**ネットワーク | IPSec VPN > ルールと設定**」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。

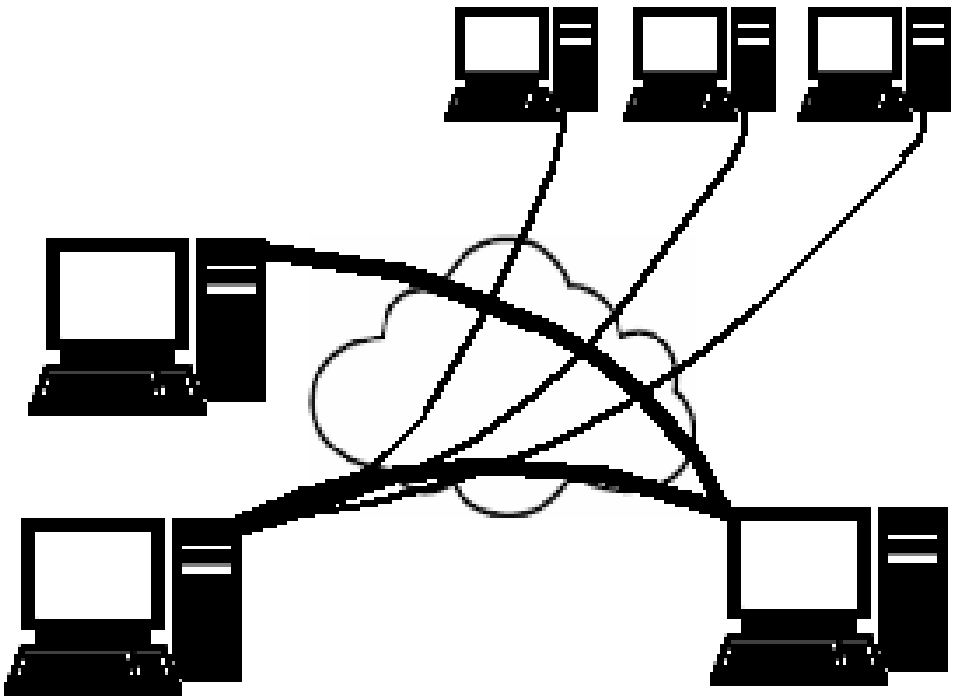
トピック:

- 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提供されます。

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。たとえば、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付け。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/X 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、主に「**ネットワーク | IPSec VPN > ルールと設定**」と「**ネットワーク | IPSec VPN > 詳細設定**」で設定します。

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 は、ポリシーベース VPN（サイト間）、ルートベース VPN トンネル、レイヤ 2 トンネリング プロトコル（L2TP）を作成するために使用できます。

VPN を越えた DHCP

SonicOS/X 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、一つ以上の 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。

ⓘ **補足:** SonicWall で製造している Secure Mobile Access (SMA) 装置は、SonicOS/X が動作する SonicWall ネットワーク セキュリティ装置と連携させて使うことも、別個に使うことも可能です。SonicWall SMA 装置の詳細は、https://www.sonicwall.com/ja-jp/products/remote-access/remote-access-appliances 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/X は、IKE の 2 つのバージョンをサポートしています。

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タイプです。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 RFC 4306 に記載されています。これは、http://www.ietf.org/rfc/rfc4306.txt で閲覧できます。

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. 開始側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) を開始側が送信する
    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. 開始側が識別情報 (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開始側が提案すると、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。 たとえば、次のようになります。
    1. 開始側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. 開始側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 タイプです。

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	• 接続を確立するための、より少ないメッセージ交換
• より高い信頼性	• EAP 認証サポート
• より簡易化	• MOBIKE サポート
• より高速	• ビルトイン NAT トラバーサル
• 拡張性	• 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、ハウスキーピングのオーバーヘッドを軽減します。

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、ユーザはラップトップの接続を切断して 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 (必要に応じて)、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/X 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	• AES-128	• AESGCM16-128	• AESGMAC-128
• 3DES	• AES-192	• AESGCM16-192	• AESGMAC-192
• なし	• AES-256	• AESGCM16-256	• AESGMAC-256

SonicOS/X は、次の**認証**方式をサポートしています。

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

Suite B 暗号化について

SonicOS/X 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。

詳細については、「**ネットワーク | IPSec VPN > ルールと設定**」ページにある以下の項目を参照してください。

- ポリシー
- アクティブ トンネル
- 設定

「IPSEC VPN > ルールと設定」ページ

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。

ⓘ **補足:** 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) ウィンドウの左上でバージョン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。

ポリシー

すべての定義済 VPN ポリシーは、「**ネットワーク | IPSec VPN > ルールと設定**」の「**ポリシー**」タブに表示されます。

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。
- 「**構成**」 – 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。

「**ポリシー**」テーブルの下には以下のボタンがあります。

検索	特定の VPN ポリシーを見つけるために利用できる標準検索エンジン。
+ 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 GroupVPN ポリシー以外）をすべて削除します。

ⓘ **補足:** 「**ポリシーにリンクを追加**」および「**ポリシーにリンクしているのでリンクを削除**」テーブルの上部にある「**再表示**」オプションを使用することにより、アクティブ トンネルを再表示することができます。

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「**構成**」列で「**編集**」アイコンをクリックすると、GroupVPN ポリシーを構成するための「**セキュリティ ポリシー**」ウィンドウが表示されます。

ⓘ **補足:** 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。

アクティブ 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。

検索	特定のアクティブ トンネルを見つけるために利用できる標準検索エンジン。
作成日	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
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

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

設定

「**ネットワーク | IPSec VPN > ルールと設定**」ページの「**設定**」タブには、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。
一意の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。

IPv6 VPN の設定

IPv6 用のサイト間 VPN の設定は、「**ネットワーク | IPSec VPN > ルールと設定**」ページの「**IPv6**」タブで、IPv4 VPN と同様の手順で行えます。

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**」画面で:
  - 「**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**」画面で:
  - 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「**ローカル ネットワーク**」および「**リモート ネットワーク**」で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

ⓘ **補足:** 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 アドレスが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ー
10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0ー
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 > 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ー
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。

ⓘ **補足:** 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。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、「**デバイス | ユーザ > ローカル ユーザ & グループ > ローカル ユーザ > ユーザの追加 > VPN アクセス**」を選択します。

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。たとえば、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、https://www.sonicwall.com/ja-jp/support/video-tutorials でご覧いただけます。

ⓘ **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。個別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」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. 「**ネットワーク | IPSec VPN > ルールと設定**」ページに移動します。
2. IPv4 または IPv6 のどちらか適切なバージョンを選択します。
3. 「**+ 追加**」をクリックします。
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**」の各タブで必要な設定を行います。以下のセクションで、それらの個々のタブに関する追加情報を提供します。

トピック:

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

「一般」タブでの設定

「**一般**」タブで、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。
   ⓘ | **補足:** 「**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 メニューから認証方式を選択します。「**一般**」タブ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。
   ⓘ | **補足:** 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」タブでの設定

「**ネットワーク**」タブで、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**」タブで、「**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 はサポートされないため、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」タブでの設定

「**プロポーザル**」タブでは、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、選択内容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。

IPV4 での VPN ポリシーの追加: プロポーザル

「詳細」タブでの設定

IPv4 と IPv6 の「**詳細**」タブは似ていますが、一部のオプションはどちらか一方でのみ使用できます（「詳細設定: オプション利用可能性」を参照）。また、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	–
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

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

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 アドレスが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

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、「**オブジェクト | 一致オブジェクト > ゾーン | + ゾーンの追加**」に移動してください。

SonicOS/X 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。以下の既定の GroupVPN ポリシーが、「**ネットワーク | IPSec VPN > ルールと設定**」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

補足: 工場出荷時の既定の設定の SonicOS/X 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/X 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 ポリシーのダウンロード

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. 「**ネットワーク | IPSec VPN > ルールと設定**」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**」タブにおいて、「**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。

ⓘ | **補足:** 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。
     ⓘ | **補足:** 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**」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 モード構成を有効にする	SonicOS/X 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。 **補足:** 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

詳細設定	
	トは破棄されます。
クライアント認証	
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を許可する	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/X 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。 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。
次への接続を許可する	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。 • 「**トンネル分割**」を使用すると、VPN ユーザはローカル インターネット接続と VPN 接続の両方を使用できます。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、関係するユーザが自分のために設定されたネットワークだけをアクセスできるようになります。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**」をクリックします。
11. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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

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. 「**ネットワーク | IPSec VPN > ルールと設定**」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。
   ⓘ | **補足:** VPN ポリシー名は、既定で「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 ID**」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ピア証明書のみ許可する**」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。

ⓘ | **補足:** 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**」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 モード構成を有効にする	SonicOS/X 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 1 つ以上選択します。 ⓘ | **補足:** 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 トラフィックを送信する**」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ため、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 トンネル経由で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」および「OCSP 応答 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 ユーザに対するユーザ 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を許可する	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。 • 「**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/X 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。
次への接続を許可する	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。 ⓘ **補足:** 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。 • 「**トンネル分割**」を使用すると、VPN ユーザはローカル インターネット接続と VPN 接続の両方を使用できます。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] をクリックします。
16. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」を選択して、VPN ポリシーを更新します。

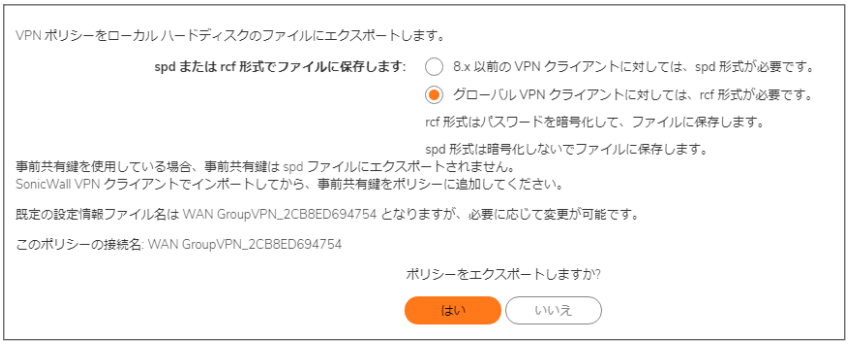
GroupVPN クライアント ポリシーのダウンロード

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ダウンロードしてください。

ⓘ **重要:** 設定ファイルをダウンロードするには、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ダウンロードするには、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」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「**構成**」列にある「**ダウンロード**」アイコンを選択します。



既定では「**SonicWall 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 メニューから、「**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. 「**送信**」をクリックします。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**] をクリックします。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。

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 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

ⓘ **補足:** 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、https://www.sonicwall.com/ja-jp/support/video-tutorials でご覧いただけます。

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. 「**ネットワーク | IPSec VPN > ルールと設定**」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. 「**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、「**共有鍵**」と「**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、「**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、「**共有鍵を隠す**」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。 ⓘ | **補足:** 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。 ⓘ | **補足:** 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。 ⓘ | **補足:** このオプションは、「**プロポーザル**」タブで「**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。 ⓘ | **補足:** このオプションは、「**プロポーザル**」タブで「**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。 ⓘ **補足: 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**」の既定値はほとんどの VPN 設定に使用できます。

ⓘ **補足:** 「**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。

ⓘ **補足:** 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。

5. 「**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。

ⓘ | **補足:** 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。

18. 「**詳細**」を選択します。

19. 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（以下のメイン モードおよびアグレッシブ モードの「詳細設定」の図を参照）**	**IKEv2 モード（以下の IKEv2 モードの「詳細設定」の図を参照）**
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後で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。	IKEv2 モードでは選択できません。

オプション	メイン モードまたはアグレッシブ モード（以下のメイン モードおよびアグレッシブ モードの「詳細設定」の図を参照）	IKEv2 モード（以下の IKEv2 モードの「詳細設定」の図を参照）
詳細設定		
	ⓘ **補足:** 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。	
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アクセス ルール コントロール」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アクセス ルール コントロール」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。
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	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、

オプション	メイン モードまたはアグレッシブ モード（以下のメイン モードおよびアグレッシブ モードの「詳細設定」の図を参照）	IKEv2 モード（以下の IKEv2 モードの「詳細設定」の図を参照）
詳細設定		
	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。 ⓘ **補足:** 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。	「**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。 ⓘ **補足:** 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。
この SA を経由しての管理	ローカル 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 SonicWall」のいずれかを選択します。	ローカル 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 SonicWall」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。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。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。たとえば、（「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。たとえば、（「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 メニュー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	ドロップダウン メニュー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

オプション	メイン モードまたはアグレッシブ モード（以下のメイン モードおよびアグレッシブ モードの「詳細設定」の図を参照）	IKEv2 モード（以下の IKEv2 モードの「詳細設定」の図を参照）
詳細設定		
	す。重要: VPN ゲートウェイの IP アドレスが両方で同じ場合、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。	同じ場合、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、IKE ピアによってはトリガー パケットを含めないのが適切な場合があります。
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。

20. 「**OK**」をクリックします。
21. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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（たとえば、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）を使用する VPN ポリシーを設定するには、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」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「**手動鍵**」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。
     ⓘ | **補足:** 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より選択**」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 メニューから値を選択してください。

    ⓘ | **補足:** 「**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。たとえば、1234567890abcdef は有効な DES または ARCFour 暗号キーの例です。不適切な暗号キーまたは認証キーを入力すると、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**」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アクセス ルール コントロール」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。 ⓘ **補足:** 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。

オプション	定義
	ⓘ **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、https://www.sonicwall.com/ja-jp/support/video-tutorials でご覧いただけます。
この SA を経由しての管理	ローカル **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」、「SNMPSonicWall」、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。 ⓘ **補足:** 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。たとえば、(「**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 メニュー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、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**」をクリックします。
17. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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

ⓘ **補足:** 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. 「**ネットワーク | IPSec VPN > ルールと設定**」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. 「SonicWall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** 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

ピア IKE ID 種別オプション	定義
	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 ID (ユーザ FQDN)** 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 (FQDN)** 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。

ⓘ **補足:** 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、「**デバイス | 設定> 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。

  ⓘ **補足:** 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より選択**」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 メニューから選択します。
- 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 メニュー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。 ⓘ **補足: 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。

ⓘ **補足:** 「**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。

ⓘ | **補足:** 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。

ⓘ | **補足:** 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**」を選択します。

20. VPN ポリシーに適用する設定オプションを選択します。

詳細設定

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
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後で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。	IKEv2 モードでは選択できません。

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
	ⓘ **補足:** 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。	
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アクセス ルール コントロール」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アクセス ルール コントロール」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。
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	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

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
	ニューから 1 つずつを選択してください。 ⓘ **補足:** 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。	を選択してください。 ⓘ **補足:** 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。
この SA を経由しての管理	ローカル **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」、「SNMPSonicWall」、またはこの 3 つを組み合わせて選択します。	ローカル **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」、「SNMPSonicWall」、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。 ⓘ **補足:** 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。 ⓘ **補足:** 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、「**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 メニュー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、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 メニュー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、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
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、IKE ピアによってはトリガー パケットを含めないのが適切な場合があります。
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**」をクリックします。
22. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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. 「**ネットワーク | IPSec VPN > ルールと設定**」に移動します。
2. 「**+ 追加**」をクリックします。「**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**」を選択します。

4. 「**名前**」フィールドに装置の名前を入力します。
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。

     ⓘ **補足:** 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より選択**」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。

    ⓘ **補足:** 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。

    ⓘ **補足:** 「**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。たとえば、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**」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。

  ⓘ **補足:** 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。

  ⓘ **補足:** 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**」をクリックします。
17. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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。

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. 「**ポリシー | ルールとポリシー > ルーティング ルール**」に移動します。
2. 「**+ 追加**」を選択します。

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。
   ポリシー ルールを見つけやすくするため、最大 3 つの「**タグ**」を入力します。区切り文字としてカンマを使用します。
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. 「**保存**」をクリックします。

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/X 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。

- VPN 自動プロビジョニングの定義
- 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仕組み

VPN 自動プロビジョニングの定義

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。

ⓘ **補足:** 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、SonicOS/X 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 SonicWall 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仕組み

VPN 自動プロビジョニングは 2 段階で動作します。

- 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「**ネットワーク | IPSec VPN > ルールと設定**」ページで VPN ポリシーを追加することにより行います。

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。

ⓘ **補足:** 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 セキュリティに欠かせない以下の要素を備えています。

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、対象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。

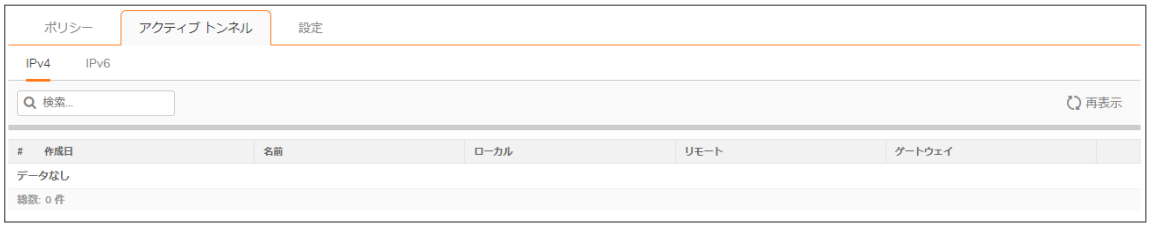
フェーズ 1 SA の確立とポリシー プロビジョニングの完了後、対象先ネットワークが「**ネットワーク | IPSec VPN > ルールと設定**」ページの「**VPN ポリシー**」セクションに表示されます。

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」での VPN AP サーバの設定*」を参照）。

ⓘ **補足:** 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「アクティブ トンネル」リストに表示されます。



また、NAT ルールが「**ポリシー | ルールとポリシー > NAT ルール**」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 サーバは、SonicOS/X の「**ネットワーク | IPSec VPN > ルールと設定**」ページで VPN ポリシーを追加することにより、サーバ（ハブ）ファイアウォール上で設定されます。

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」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. 「**ネットワーク | IPSec VPN > ルールと設定**」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. 「**+ 追加**」をクリックします。「**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。

「一般」画面でのVPN APサーバの設定

VPN APサーバの「一般」を設定するには、以下の手順に従います。

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** – 次に入力する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に進みます。
   - **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。

     ⓘ **補足:** 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。このフィールドには「**名前**」フィールドに入力した値が自動的に設定されますが、変更可能です。

   ⓘ **補足:** 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クライアントを終端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**」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クライアントに対してプロビジョニングされます。

   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。

   ⓘ **補足:** 最高のセキュリティを得るために、SonicWallでは、VPN APクライアントがその共有鍵でプロビジョニングを行い、管理社の精査が可能な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、「**共有鍵**」フィールドに何らかの入力を行う前に、「**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、「**共有鍵**」フィールドの値が「**共有鍵の確認**」フィールドに自動的にコピーされます。
6. 「**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**」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VPN APクライアントに対してプロビジョニングされます。「**既定のプロビジョニング鍵を使用する**」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. 「**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「**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に進みます。

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 ID 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」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、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」ページに移動します。
2. 「**IP バージョン**」として「**IPv4**」を選択します。
3. 「**+ 追加**」をクリックします。「**VPN ポリシー**」ダイアログが表示されます。
4. 「**一般**」タブの「**認証方式**」で、「**SonicWall 自動プロビジョニング サーバ**」を選択します。
5. 「**ネットワーク**」タブを選択します。

6. 「**ローカル ネットワーク**」の下で、「**XAUTH を利用した VPN AP クライアントの認証を要求する**」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。
7. 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「**デバイス | ユーザ > 設定 | ユーザ認証方式**」で設定されている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。
8. 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を許可する**」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。
9. 「**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より選択** – 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。

ⓘ **補足:** 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。

  ⓘ **補足:** 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。

  ⓘ **補足:** 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。

10. 続きは「*「プロポーザル」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、以下の手順に従います。

1. 「**一般**」または「**ネットワーク**」タブで、「**プロポーザル**」を選択します。

2. 「**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**

3. 「**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。

4. 「**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。

5. 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。選択した場合、「**DH グループ**」ドロップダウン メニューが表示されます。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。

6. 「**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。

7. 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、以下の手順に従います。

1. 「**詳細**」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**」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**」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 メニュー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. 「**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。
7. 「**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。
8. 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。

   ⓘ | **補足:** このオプションは、一部のバージョンの SonicOS/X で機能しない可能性があります。
9. 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。
10. 終了したら、「**保存**」を選択します。

VPN AP クライアントの設定

VPN AP クライアントは、SonicOS/X の「**ネットワーク | IPSec VPN > ルールと設定**」ページで VPN ポリシーを追加することにより、クライアント ファイアウォール上で設定されます。

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 ファイアウォールを設定するには、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」ページに移動します。
2. IP バージョンとして「**IPv4**」を選択します。
3. 「**+ 追加**」をクリックします。「**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 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** – 次に入力する 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 に進みます。
   - **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**として設定された SonicWall ファイアウォール）の設定によって決定されます。

ⓘ **補足:** 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**」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 クライアントに対してプロビジョニングされます。

ⓘ **補足:** 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**」を選択しなかった場合は、必要に応じて、「**共有鍵**」フィールドに何らかの入力を行う前に、「**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、「**共有鍵**」フィールドの値が「**共有鍵の確認**」フィールドに自動的にコピーされます。
11. 「**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. 「**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「**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 に移動してください。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、「**保存**」を選択して、VPN ポリシーを追加します。

4

ルールと設定

ここでは、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」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:

- トンネル インターフェースの追加
- 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
- 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、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」に移動します。
2. 「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**」をクリックします。

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。オプションが次のように変化します。
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
   - 事前共有鍵を使用する設定
   - サードパーティ証明書を使った設定
   - VPN AP クライアントの設定
   - VPN AP サーバの設定

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。 ⓘ **補足:** 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**」の既定値はほとんどの VPN 設定に使用できます。

   ⓘ **補足:** 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

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
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。

ⓘ | **補足:** 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

ⓘ | **補足:** 「**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 メニュー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**」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）。

詳細設定

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
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	システム > 動的ルーティング**」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	システム > 動的ルーティング**」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。
	補足: 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	

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
	(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。
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。 ⓘ **補足:** 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。 ⓘ **補足:** 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。
この SA を経由しての管理	ローカル **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」、	ローカル **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 SonicWall」

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
	「SNMP SonicWall」のいずれかを選択します。	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。 ⓘ **補足:** 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。 ⓘ **補足:** 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 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、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 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、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。

IKEV2 設定

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
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、IKE ピアによってはトリガー パケットを含めないのが適切な場合があります。
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. 「**保存**」をクリックします。
13. 「**ネットワーク | IPSec VPN > ルールと設定**」ページで、「**適用**」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、以下の手順に従います。

1. 「**ネットワーク | IPSec VPN > ルールと設定**」に移動します。
2. 「**+ 追加**」をクリックして、「VPN ポリシー」ダイアログを表示します。
3. 利用可能なすべてのトンネル インターフェースが表示される「**ポリシー種別**」ドロップダウン メニューから、「**トンネル インターフェース**」を選択します。

   ⓘ **補足:** 「**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。
5. 「**保存**」をクリックします。

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。

5

詳細

「**ネットワーク | IPSec VPN > 詳細設定**」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。
    - **Dead peer 検出間隔** – "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。規定値は 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。
    - **無動作の 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、無条件に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 デバイスがある場合は、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る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クリーンアップする** – 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**
        - XAUTH 用 **MSCHAPv2** モード (ユーザに期限切れパスワードの変更を許可する)

また、これを設定し、「**デバイス | 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。

ⓘ | **補足:** 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 (Novell eDirectory) を使用している。

- **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 サーバ設定を構成するには、「**構成**」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。

- **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 サーバを指定する** – 「**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/X では、IKEv2 動的クライアントのサポートにより、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。
  「**構成**」を選択すると、「**IKEv2 動的クライアント プロポーザルの構成**」ダイアログが表示されます。

SonicOS/X 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。

ⓘ | **補足:** 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すことができます。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。頻繁にアップデートが必要になると、各クライアントにより完全な 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2～3個程度の証明書を確認するだけなので、その数個の証明書のエントリのために CRL 全体をダウンロードするという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ることができません。

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/X 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. 「**デバイス | 設定 > 証明書**」ページで、「**インポート**」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。

VPN ポリシーでOCSP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**」を選択します。
2. OCSP サーバの「**OCSP 応答 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

「**ネットワーク | IPSec 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**) 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**) 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. 「**ネットワーク | IPSec VPN >VPN を越えた DHCP**」を選択します。
2. 「**ゲートウェイ**」ドロップダウン メニューから、「**セントラル**」を選択します。
3. 「**構成**」をクリックします。

4. 次のいずれかを選択します。
   - グローバル VPN クライアントまたはリモート ファイアウォール、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。

1. 「**+ 追加**」をクリックします。
2. 「**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。
3. 「**OK**」をクリックします。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**」をクリックします。

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. 「**ゲートウェイ**」ドロップダウン メニューから、「**リモート**」を選択します。
2. 「**構成**」をクリックします。

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。

> ⓘ **補足:** 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. 「**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。

   > ⓘ **補足:** 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。

6. 「**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 をリモートで管理するためにも使用されます。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。
7. 「**IP Spoof 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。
8. 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った後で、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」を有効にします。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。
9. 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。
10. LAN の機器を設定するには、「**デバイス**」を選択します。

11. 「**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。

12. 「**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 アドレスのブロックを確保しておくことをお勧めします。

13. 「**OK**」をクリックします。

14. 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。
15. 「**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。
16. 「**OK**」をクリックします。
17. 「**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。

ⓘ **補足:** 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。

ⓘ **補足:** 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。

ⓘ **補足:** 無線クライアントには、このサブネット内の IP アドレスが割り当てられます。IP アドレスと DHCP サーバが自動的に作成され、DHCP アドレスが割り当てられます。

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「**構成**」により、テーブル エントリ (バインド) を構成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

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:

- L2TP サーバの設定
- 現在動作中の L2TP セッションの表示
- Microsoft Windows L2TP VPN クライアント アクセスの設定
- Google Android L2TP VPN クライアント アクセスの設定

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

L2TP サーバの設定

「**ネットワーク | IPSec 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. 「**ネットワーク | IPSec 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**」を選択します。「**構成**」が使用可能になります。
3. 「**構成**」を選択して、「**L2TP サーバ構成**」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。 ⓘ **補足:** このオプションを使用するためには、「**デバイス | 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 ユーザのユーザ 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**」をクリックします。

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

ここでは、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。

ⓘ **補足:** SonicOS/X 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/X 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. 「**ネットワーク | VPN > ルールと設定**」ページに移動します。
2. **WAN GroupVPN** ポリシーの場合は、「**構成**」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. 「**共有鍵**」フィールドに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. 「**保存**」をクリックします。
6. 「**ネットワーク | IPSec VPN > L2TP サーバ**」ページに移動します。
7. 「**L2TP サーバ**」セクションで、「**L2TP サーバを有効にする**」を選択します。
8. 「**構成**」をクリックします。
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 ユーザ設定**」を選択します。
11. 以下のオプションを設定します。
    - RADIUS/LDAP サーバが IP アドレス情報を L2TP クライアントに提供する場合は、「**RADIUS/LDAP サーバにより提供された IP アドレス**」。L2TP サーバが IP アドレスを提供する場合は、「**ローカル L2TP IP プールを使用する**」を選択します。
    - **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 (独自 IP を使用)
    - **終了 IP アドレス**: 10.20.0.20 (独自 IP を使用)
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. 「**保存**」をクリックします。
14. 「**デバイス | ユーザ> ローカル ユーザ & グループ**」に移動します。
15. 「**ローカル ユーザ**」を選択します。
16. 「**+ ユーザの追加**」をクリックして「**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. 「**保存**」をクリックします。

ⓘ **補足:** VPN > LAN アクセス ルールまたは別の VPN アクセスルール(「**ポリシー | ルールとポリシー > 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「**すべての種別**」表示を選択し、「**L2TP IP プール**」の「**送信元**」列を確認します。

a. 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。
b. 「**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。
c. **新しい接続ウィザード**を開きます。
d. 「**職場に接続**」を選択します。
e. 「**次へ**」を選択します。
f. 「**仮想プライベート ネットワーク接続**」を選択します。「**次へ**」を選択します。
g. VPN 接続の名前を入力します。「**次へ**」を選択します。
h. 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。
i. 「**次へ**」を選択し、「**完了**」を選択します。
j. 「接続」ウィンドウで「**プロパティ**」を選択します。
k. 「**セキュリティ**」を選択します。
l. 「**IPSec 設定**」を選択します。
m. 「**認証に事前共有鍵を使用する**」を有効にします。

n. 事前共有鍵を入力し、「**OK**」を選択します。
o. 「**ネットワーク**」を選択します。
p. 「**VPN の種類**」を「**自動**」から「**L2TP IPSec VPN**」に変更します。
q. 「**OK**」をクリックします。
r. XAUTH ユーザ名およびパスワードを入力します。
s. 「**接続**」を選択します。

19. 「**ネットワーク | IPSec VPN > ルールと設定**」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

ここでは、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. 「**ネットワーク | IPSec VPN > ルールと設定**」ページに移動します。
2. **WAN GroupVPN** ポリシーの場合は、「**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. 「**共有鍵**」フィールドに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**」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**」をクリックします。
13. 「**ネットワーク | IPSec 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**」を選択します。
15. 「**構成**」をクリックします。
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 (または独自 IP を使用)
    - **終了 IP**: 10.20.0.20 (または独自 IP 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. 「**保存**」をクリックします。
21. 「**デバイス | ユーザ> ローカル ユーザ & グループ**」に移動します。
22. 「**ローカル ユーザ**」を選択します。
23. 「**+ ユーザの追加**」をクリックします。
24. 「**設定**」画面で、ユーザの「**名前**」と「**パスワード**」を指定します。
25. 「**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。

    ⓘ **補足:** 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。

    ⓘ **補足:** これで、SonicOS/X 設定が完了しました。

26. 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 GroupVPN 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。

27. 「**ネットワーク | IPSec VPN > ルールと設定**」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/jp/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、「**ネットワーク | システム > 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、「**ネットワーク | IPSec VPN > AWS VPN**」に移動します。「**AWS VPN**」ページの中心となる部分は、対象となる 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。

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、このファイアウォールを接続したい Amazon VPC の該当する行の「**VPN 接続の作成**」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。

ⓘ **補足:** 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、*ルート伝搬*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、「**ネットワーク | IPSec 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」をクリックします。

ⓘ **補足:** 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**pending**として報告されます。「AWS VPN」ページの「再表示」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/X 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。「**オブジェクト | 一致 オブジェクト > アドレス**」に移動します。このオブジェクトの命名規則は、VPN 接続の AWS ID と VPC 自体の AWS ID が組み合わされた名前となります。このアドレス オブジェクトの種別はネットワークで、リモート VPC のネットワークのものとなります。

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。「**ネットワーク | IPSec VPN > ルールと設定**」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。「**ネットワーク | システム > 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。「**ネットワーク | システム > 動的ルーティング**」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。

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、対象のサブネットで使われているルート テーブルにその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 テーブルでは伝搬が可能ですが、そうでないルートテーブルもあるからです。
- 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、制御するルート 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、「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、以下の手順に従います。

1. 対象のルート テーブルを選択します。
2. 「**ルート伝搬**」タブを選択します。
3. 「**編集**」を選択します。
4. 必要に応じて、「**伝搬**」チェックボックスをオンまたはオフにします。
5. [**保存**] 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、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に実行できる限り多く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。

9

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、次の URL を開きます。
https://www.sonicwall.com/ja-jp/support

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。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする。
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com 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 サポートに連絡するには、次の URL にアクセスします。https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

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

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS および SonicOSX IPSec VPN 管理ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005442-00 Rev B

エンドユーザ製品契約

SonicWall エンドユーザ製品契約を参照する場合は、以下に移動してください。https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. 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
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035