SonicOS 7 システム

管理ガイド

SONICWALL®

内容

1

インターフェース

「**ネットワーク | システム > インターフェース | インターフェース設定**」ページには、IPv4 と IPv6 両方の物理インターフェースに直接リンクされたインターフェース オブジェクトが含まれています。SonicOS のインターフェース アドレス指定方式は、ネットワーク ゾーンおよびアドレス オブジェクトと連動しています。

IPV4 インターフェース設定

IPV6 インターフェース設定

トピック:

- インターフェースについて
- IPv4 のインターフェース設定
- 31 ビット ネットワーク設定
- PPPoE アンナンバード インターフェースのサポート

インターフェースについて

トピック:

- 物理インターフェースと仮想インターフェース
- SonicOS のセキュリティ保護されるオブジェクト
- トランスペアレント モード
- IPS スニッファ モード
- Firewall Sandwich
- HTTP/HTTPS リダイレクト
- インターフェースでの DNS プロキシの有効化
- LTE モデムのサポート
- LAN バイパス

物理インターフェースと仮想インターフェース

SonicOS のインターフェースは大きく次のように分けられます。

- **物理インターフェース** — 物理インターフェースは、単一のポートにバインドされます。
- **仮想インターフェース** — 仮想インターフェースは、サブインターフェースとして物理インターフェースに割り当てられ、複数のインターフェースに割り当てられたトラフィックを物理インターフェースが搬送できるようにします。

トピック:

- 物理インターフェース
- 仮想インターフェース (VLAN)
- サブインターフェース

物理インターフェース

SonicWall セキュリティ装置のフロント パネルには多くの物理インターフェースがあります。インターフェースの数と種類は装置のモデルとバージョンによって異なります (お使いの装置のインターフェースの詳細は、その装置の『*クイック スタート ガイド*』を参照してください)。

物理インターフェースは、送受信トラフィックを規定するアクセス ルールの設定が可能なゾーンに割り当てる必要があります。セキュリティ ゾーンは、送受信トラフィックの経路として動作する各物理インターフェースにバインドされます。インターフェースがなければ、トラフィックはゾーンにアクセスしたり、ゾーンを出ていくことができません。

ゾーンの詳細については、「*ゾーンについて*」を参照してください。

仮想インターフェース (VLAN)

仮想インターフェースは、物理インターフェースに割り当てられたサブインターフェースであり、SonicWall セキュリティ装置でサポートされます。仮想インターフェースにより、1 つの物理接続で複数のインターフェースを使用できます。

仮想インターフェースは、ゾーンの割り当て、DHCP サーバ、NAT、アクセル ルールの管理など、物理インターフェースと同じ機能を数多く備えています。

仮想ローカル エリア ネットワーク（VLAN）は、IP ヘッダーのタグ付けを使用することで、単一の物理 LAN の中で複数の LAN をシミュレートできるため、“タグベースの LAN 多重テクノロジ”と表現できます。物理的に個別の、接続されていない 2 つの LAN は、互いに完全に分かれています。2 つの異なる VLAN についても同様ですが、VLAN の場合、2 つの VLAN は、同じ回線上に存在できます。VLAN では、このような仮想化を実現する VLAN 対応のネットワーキング機器が必要です。これらは、ネットワークの設計とセキュリティ ポリシーに従って VLAN タグ（ID）を認識、処理、削除、および挿入できるスイッチ、ルータ、およびファイアウォールです。

VLAN は多くのさまざまな理由で役立ちますが、その理由の多くは、VLAN が、物理的ではなく論理的なブロードキャストドメイン、つまり LAN 境界を提供できる機能に基づいています。これは、大きな物理 LAN を複数の小さな仮想 LAN に分割する場合と、物理的に異なる複数の LAN を論理的に連続する 1 つの仮想 LAN にまとめる場合の、両方に該当します。この利点は、以下のとおりです。

- **性能の向上** — 論理的に分割された小さなブロードキャストドメインを作成することで、必要な送信先にのみブロードキャストを送信し、アプリケーション トラフィック用に多くの帯域幅を残せるため、ネットワーク全体の使用率が低下します。
- **コストの減少** — ブロードキャストのセグメント化は、かつてはルータで行われていたため、新たなハードウェアと設定が必要でした。VLAN では、ルータの機能的な役割は一変しました。通信の抑制目的で使用されるのではなく、必要に応じて、異なる VLAN 間の通信を促進するために使用されます。
- **仮想ワークグループ** — ワークグループは、マーケティング部門やエンジニアリング部門など、一般に情報を共有する論理単位です。効率上の理由で、ブロードキャストドメイン境界は、このような機能ワークグループに対応するように作成する必要がありますが、それが常に可能であるとはかぎりません。エンジニアリング ユーザとマーケティング ユーザが建物の同じ階（および同じワークグループ スイッチ）を共有していて、入り混じっていることもあれば、その逆にエンジニアリング チームが、構内全体に分散していることもあります。この状態を複雑な配線を駆使して解決するのはコストがかかり、絶えず行われる追加や移動を保守するのは不可能です。VLAN では、スイッチを簡単に再設定して、論理的なネットワーク配置をワークグループの要求に対応させることができます。
- **セキュリティ** — ある VLAN 上のホストは、別の VLAN 上のホストと、両者間の通信を促進するネットワーク機器がなければ通信できません。

サブインターフェース

SonicOS の VLAN サポートは、物理インターフェースの下にネストされる論理インターフェースである、サブインターフェースを使用して実現されます。一意のタグごとに、独自のサブインターフェースが必要です。セキュリティと管理上の理由で、SonicOS は VLAN トランク プロトコルに対応していません。代わりに、サポートされる各 VLAN を設定し、適切なセキュリティ機能を割り当てる必要があります。

ⓘ **補足:** VLAN ID の範囲は 0 ～ 4094 です。ただし、VLAN 0 は QoS 用に予約されており、VLAN 1 はネイティブ VLAN 指定用に一部のスイッチに予約されています。

ⓘ **補足:** ファイアウォールに接続している他の機器からのトランク リンクで、VTP（VLAN Trunking Protocol）や GVRP（Generic VLAN Registration Protocol）などの動的な VLAN トランク プロトコルを使用しないでください。

VLAN ケーブル スイッチからのトランク リンクは、関連する VLAN ID をファイアウォール上のサブインターフェースとして宣言し、それらを、物理インターフェースを設定する方法とほぼ同じ方法で設定することにより、サポートされます。言い換えると、サブインターフェースとして定義された VLAN だけがファイアウォールによって処理され、それ以外は対象外として破棄されます。この方法の場合、トランク リンクの接続先であるファイアウォール上の親物理リンクは従来のインターフェースとして動作し、同じリンク上に存在する可能性があるネイティブの（タグ付きでない）VLAN トラフィックもサポートできます。また、親インターフェースは、“未定義”のままです。

VLAN サブインターフェースは、ゾーンの割り当て、セキュリティ サービス、GroupVPN、DHCP サーバ、IP ヘルパー、ルーティング、NAT ポリシーとアクセス ルールの完全な制御など、物理インターフェースの大部分の機能と特徴を備えています。マルチキャスト サポートは、現時点では VLAN サブインターフェースから除外されています。

SonicOS のセキュリティ保護されるオブジェクト

SonicOS のインターフェース アドレス指定方式は、アドレス オブジェクト、サービス オブジェクト、およびネットワーク ゾーンと連動しています。この構造は、セキュリティが保護されるオブジェクトに基づいており、SonicOS 内のルールとポリシーでこれらのオブジェクトが使用されます。

セキュリティ保護されるオブジェクトには、物理インターフェースに直接リンクされ、「**ネットワーク | システム > インターフェース**」ページで管理されるインターフェース オブジェクトが含まれます。アドレス オブジェクトとサービス オブジェクトは、それぞれ「**一致オブジェクト > アドレス**」と「**一致オブジェクト > サービス**」で定義されます。

ゾーンは、SonicOS のセキュリティ保護されたオブジェクトの手法の、階層上の頂点にあたります。SonicOS には事前に定義されたゾーンがあり、これとは別に独自のゾーンを定義することもできます。事前定義ゾーンは、LAN、WAN、DMZ、VPN、SSLVPN、マルチキャスト、およびユーザ定義です。ゾーンに関する詳細は、「ネットワーク ゾーンの設定」を参照してください。

ゾーンには複数のインターフェースを指定できます。ただし、WAN ゾーンは最大でインターフェースの合計数マイナス 1 に制限されています。「**ネットワーク | システム > フェイルオーバー & 負荷分散**」での WAN フェイルオーバーと負荷分散の設定に応じて、WAN ゾーン内では、1 つまたは複数の WAN インターフェースがアクティブにトラフィックを搬送できます。SonicWall セキュリティ装置における WAN フェイルオーバーおよび負荷分散の詳細については、「フェイルオーバーと負荷分散」.

ゾーン設定レベルでは、ゾーンの「**インターフェース間通信を許可する**」設定により、許可を指示するゾーン内アクセス ルールの作成に関する処理が自動的に行われます。ゾーン全体の総合的なアドレス オブジェクトと、ゾーン アドレスからゾーン アドレスへの許可を包括的に指示するアクセス ルールが作成されます。

トランスペアレント モード

SonicOS のトランスペアレント モードは、インターフェースが管理階層のトップ レベルにあるものと見なすモードです。トランスペアレント モードは、一意のアドレス指定およびインターフェース ルーティングをサポートします。

IPS スニッファ モード

トピック:

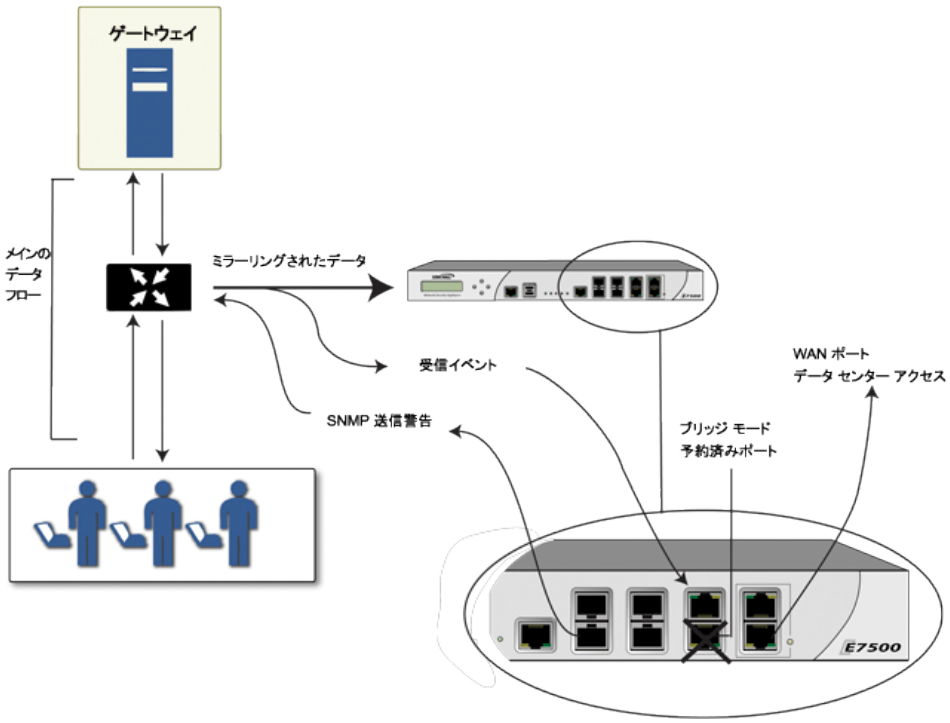
- IPS スニッファ モードのサンプル トポロジ

IPS スニッファ モードは、SonicWall セキュリティ装置でサポートされており、侵入検知に使用されるレイヤ 2 ブリッジ モードの一種です。IPSスニッファ モードを設定して、装置のインターフェースをスイッチ上のミラーリングされたポートに接続してネットワーク トラフィックを検査できます。一般に、メイン ゲートウェイ内部のスイッチでイントラネットのトラフィックを監視する目的でこのモードを使用します。

「IPS スニッファ モード: ネットワーク図」では、ローカル ネットワーク内のスイッチに流れ込んだトラフィックがスイッチのミラー ポートでミラーリングされ、装置の IPS スニッファ モード インターフェースに送られます。装置では、ブリッジ ペアで構成された設定に従ってパケットが検査されます。警告が発行されると、SNMP トラップが装置の別のインターフェースから指定の SNMP マネージャに送信されます。装置で検査されたネットワーク トラフィックは、検査終了後に破棄されます。

装置の WAN インターフェースは、ファイアウォール データ センターに接続してシグネチャ更新やその他のデータを取得するために使用されます。

IPS スニッファ モード: ネットワーク図



IPS スニッファ モードでは、レイヤ 2 ブリッジが、装置上の同じゾーンにある 2 つのインターフェース（LAN–LAN、DMZ–DMZ など）の間に設定されます。個別ゾーンを作成してレイヤ 2 ブリッジに使用することもできます。

WAN ゾーンだけは、IPS スニッファ モードでの使用に適して**いません**。その理由は、SonicOS は LAN–LAN トラフィックのような同じゾーン内のトラフィックのすべてのシグネチャを検出しますが、方向固有の（クライアント側対サーバ側）シグネチャの中には一部のLAN–WAN のケースに当てはまらないものがあるからです。

レイヤ 2 ブリッジの一方のインターフェースを、スイッチのミラーリングされたポートに接続できます。ネットワークトラフィックがスイッチに到達すると、トラフィックはミラーリングされたポートにも送信され、そこから装置に渡されて厳密なパケット検査を受けます。悪意のあるイベントが認められると警告とログ入力が開始され、SNMP が有効な場合は SNMP トラップが SNMP マネージャ システムの設定済み IP アドレスに送信されます。このトラフィックは、実際にはレイヤ 2 ブリッジのもう一方のインターフェースまで進みません。IPSスニッファ モードでは、装置はネットワークトラフィックに対してインラインに配置されません。トラフィックを検査する手段を提供するだけです。

「**ネットワーク | システム > インターフェース**」ページから表示できる「**インターフェースの編集**」ダイアログには、IPS スニッファ モードを設定するときに使用する「**このブリッジ ペアのトラフィックのみスニフする**」というオプションがあります。このオプションをオンにすると、装置ではミラーリングされたスイッチ ポートから L2 ブリッジに届くすべてのパケットが検査されます。IPS スニッファ モードを使う場合、ミラーリングされたスイッチ ポートからのトラフィックがネットワークに送り返されないように「このブリッジ ペアにトラフィックをルーティングしない」オプションも選択する必要があります。

IPS スニッファ モードでインターフェースを設定する詳細な手順については、「*IPS スニッファ モードの設定*」を参照してください。

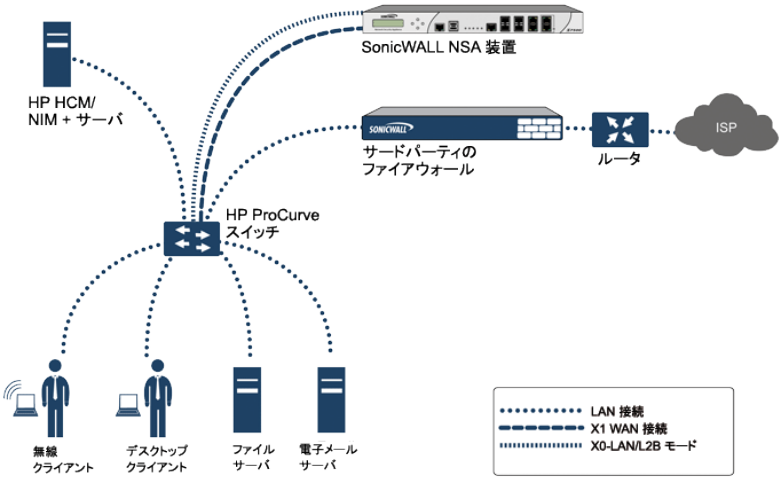
IPS スニッファ モードのサンプル トポロジ

このサンプル トポロジでは、Hewlett Packard ProCurve スイッチング環境で SonicWall IPS スニッファ モードを使用します。このシナリオは、脅威がやってくるポートを抑制したり閉じたりできる HP の ProCurve Manager Plus（PCM+）

および HP Network Immunity Manager (NIM) サーバ ソフトウェア パッケージの機能に依存しています。

この方式は、既に装置が備わっているネットワークで、装置のセキュリティ サービスをセンサーとして利用したい場合に便利です。

IPS スニッファ モード: サンプル トポロジ



この配備では、WAN インターフェースおよびゾーンを内部ネットワークのアドレス指定方式用に設定し、内部ネットワークに接続します。X2 ポートは LAN ポートにブリッジされたレイヤ 2 ですが、何にも接続されません。X0 LAN ポートは HP ProCurve スイッチ上の特別にプログラムされた第 2 のポートに設定します。この特別なポートはミラーモード用に設定します。これはすべての内部ユーザおよびサーバのポートをファイアウォールの「スニッフ」ポートに転送します。それにより、ファイアウォールは内部ネットワークの全トラフィックを分析でき、セキュリティ シグネチャをトリガするトラフィックがあれば、X1 WAN インターフェースを通じて PCM+/NIM サーバにただちにトラップするので、脅威がやってくるポートに対して処置を講じることができます。

Firewall Sandwich

SonicWall Firewall Sandwich を配備、設定して IT インフラストラクチャ全体の可用性、スケーラビリティ、管理性を高めることができます。Firewall Sandwich の配備には、次の特長があります。

- **スケーラビリティ** – 既存の装置を再利用しつつ、必要に応じてさらなるキャパシティを追加します
- **冗長性と回復力** – プライマリ コンポーネントとセカンダリ コンポーネント
- **インライン アップグレード** – システムをシャットダウンすることなく、ファイアウォールとスイッチをアップグレードします
- **一元管理** – 複数のファイアウォール クラスタとブレードのポリシーを管理します
- **フル セキュリティ サービス** – DPI-SSL の機能を含みます

Firewall Sandwich の配備および設定は、サポート対象の以下の装置とサービスによって実装できます。

- Dell Force10 シリーズ スイッチ (FTOS v9.8+ が稼働する S5000、S4810、S4048、または S6000 など)
- SonicWall サービス (すべてワイヤ モードでシングル サインオンを使用する ゲートウェイ アンチウイルス、侵入防御、ASPR、DPI-SSL、CFS など)

HTTP/HTTPS リダイレクト

トピック:

- DP のオフロードによる HTTP/HTTPS リダイレクト

セキュリティ装置の設定でユーザ認証が要求されている場合、認証されていない送信元からの HTTP/HTTPS トラフィックは SonicOS ログイン画面にリダイレクトされ、そこでユーザが資格情報を入力します。送られてくる HTTP および HTTPS トラフィックの送信元でユーザがログインしておらず、そのような 1 つ以上の送信元が新しい接続を繰り返し試みると、このリダイレクトが繰り返しトリガーされるという問題が発生します。これは、正当にアクセスの確立を試行する非ユーザ デバイスかもしれませんし、サービス妨害 (DoS) 攻撃をしかける有害なコードかもしれません。セキュリティ装置でこのような問題が発生すると、データ プレーン タスクでのリダイレクトの実行と、ウェブ サーバのスレッド タスクでのターゲット リダイレクト ページの表示の両方が影響して CP の CPU 負荷が高くなります。

この影響をできるだけ小さくするため、インターフェースを追加または編集するときは「HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する」オプションを選択するようにしてください。このオプションを有効にすると、SonicOS によって HTTP を許可するアクセス ルールがインターフェースに追加され、このルールの二次的な効果として、セキュリティ上の問題がない場合に、SonicOS で HTTPS から HTTP へのリダイレクトも可能になります。認証が必要なトラフィックをリダイレクトするときの最初の手順は、この例の 1 つです。その時点で暗号化して隠さなければならない重要なデータは存在しません。その後、CP ではなくデータ プレーン (DP) で HTTP 処理を行うことができます。

ⓘ **補足:** VPN トンネル インターフェースを追加または編集するとき、または「モード / IP 割り当て」で「ワイヤ モード (2 ポート ワイヤ)」、タップ モード (1 ポート タップ)、または「PortShield スイッチ モード」を選択したとき、このオプションを使用することはできません。

DP のオフロードによる HTTP/HTTPS リダイレクト

この機能により、セキュリティ装置を通過してアクセスするユーザにユーザ認証が必要な際に発生する HTTP/HTTPS リダイレクト要求を効果的に処理できます。認証されていないユーザの HTTP/HTTPS 要求はセキュリティ装置のログイン ページにリダイレクトされます。このページは装置自身のビルトイン ウェブ サーバによって起動します。こうしたリダイレクトは、シングル サインオン (SSO) によってユーザを識別できない、または SSO が使用されていない場合に発生します。

この機能は、ウェブ サーバと HTTP/HTTPS リダイレクト プロセスの両方の効率を高めます。また、複数のコア全体に処理が分散するデータ プレーン (DP) に対する多くのリダイレクト プロセスの負荷を軽減します。

ⓘ **補足:** この機能の構成要素は、内部の「ユーザ認証の設定」オプションで制御することができます。これには、DP でのリダイレクト処理をグローバルに有効化/無効化するオプション、リダイレクト ファイル キャッシュを消去するオプション、ウェブ サーバ用の NAT の内部ポート番号を指定するオプションなどが含まれます。内部設定の詳細については、SonicWall テクニカル サポートにお問い合わせください。

インターフェースでの DNS プロキシの有効化

DNS プロキシがグローバルで有効になっている場合、DNS プロキシを個々のインターフェースに対して有効にすることができます。これにより、この機能を異なるネットワーク セグメントで個別に有効にすることができます。インターフェースで DNS プロキシを有効にする方法については、「*DNS プロキシの有効化*」を参照してください。

LTE モデムのサポート

LTE USB モデムが SonicWall セキュリティ装置に接続されている場合、SonicOS はそのモデルを検知し、「**ネットワーク | システム > インターフェース**」ページで U0 インターフェースを表示します。このインターフェースは、既定で WAN ゾーンに属し、フェイルオーバーと負荷分散や、LTE 接続、プロファイル、詳細設定のために使用できます。

LAN バイパス

LAN バイパス モードの主な機能 (有効になっている場合):

- 再起動中に、LBP 対応インターフェース間でトラフィックを渡します。
- ファイアウォールの電源がオフの場合でも、これらの LBP 対応インターフェース間でトラフィックを渡します。

IPv4 のインターフェース設 定

トピック:

- 仮想インターフェースの追加
- ルート モードの設定
- インターフェースでの帯域幅管理の有効化
- インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定
- 無線インターフェースの設定
- WAN インターフェースの設定
- トンネル インターフェースの設定
- VPN トンネル インターフェースの設定
- リンク統合とポート冗長化の設定
- IPS スニッファ モードの装置の設定
- セキュリティ サービス (統合脅威管理) の設定
- ワイヤ モードとタップ モードの設定
- レイヤ 2 ブリッジ モード

「**インターフェース設定**」テーブルには、各インターフェースに関する次の情報がリストされます。

- **名前** – インターフェースの名前。
- **ゾーン** – 既定で LAN、WAN、および WLAN がリストされ、該当する場合は DMZ と MGMT もリストされます。ゾーンが設定されると、この列に名前がリストされます。設定されていないゾーンは「未定義」と示されています。ゾーンの上にマウスを置くと、ゾーンのプロパティが表示されます。

セキュリティ種別	ゾーンの設定時に選択されたセキュリティ種別を表示します。
メンバー インターフェース	このゾーンに割り当てられているインターフェースをリストします。
インターフェース間通信	このゾーンに対して、「**インターフェース間通信を許可する**」が有効になっているかどうかを示します。
アンチウイルス	このゾーンに対して、「**クライアント AV 強制サービスを有効にする**」および/または「**ゲートウェイ アンチウイルス サービスを有効にする**」が有効になっているかどうかを示します。
DPI SSL 強制	このゾーンに対して、「**DPI SSL 強制**」が有効になっているかどうかを示します。
GSC	このゾーンに対して「**グローバル セキュリティ クライアントを強制する**」(GSC) 保護が有効になっているかどうかを示します。詳細については、「*ゾーンでの SonicWall セキュリティ サービスの有効化*」を参照してください。
SEC	このゾーンに対して「**SonicWall 強制クライアント (SEC)**」保護が有効になっているかどうかを示します。

- **グループ** – インターフェースが負荷分散グループに割り当てられた場合は、この列に表示されます。
- **IP アドレス** – インターフェースに割り当てられた IP アドレス。
- **サブネット マスク** – サブネットに割り当てられたネットワーク マスク。
- **IP 割り当て** – 使用可能な IP 割り当て方法は、インターフェースが割り当てられるゾーンによって異なります。

  ⓘ **補足:** ワイヤ モードは、NSA 2600 以降のセキュリティ装置でのみ使用できます。

LAN	**静的 IP モード** (既定)、**トランスペアレント IP モード (L3 サブネットを結合)**、**レイヤ 2 ブリッジ モード (IP ルート オプション)**、**ワイヤ モード (2 ポート ワイヤ)**、**タップ モード (1 ポート タップ)**、**IP アンナンバード**、**PortShield スイッチ モード**、**ネイティブ ブリッジ モード**
WAN	**静的** (既定)、**DHCP**、**PPPoE**、**PPTP**、**L2TP**、**ワイヤ モード (2 ポート ワイヤ)**、**タップ モード (1 ポート タップ)**
DMZ	**静的 IP モード** (既定)、**トランスペアレント IP モード (L3 サブネットを結合)**、**レイヤ 2 ブリッジ モード (IP ルート オプション)**、**ワイヤ モード (2 ポート ワイヤ)**、

	タップ モード（1 ポート タップ）、**IP アンナンバード**、**PortShield スイッチ モード**、**ネイティブ ブリッジ モード**
WLAN	**静的 IP モード**（既定）、**PortShield スイッチ モード**、**レイヤ 2 ブリッジ モード**、**ネイティブ ブリッジ モード**
Xn への PortShield（IPv4 表示のみ）	PortShield インターフェースが設定されている場合、PortShield 割り当て

- **状況** — リンクの状況と速度。
- **有効** — 「**ネットワーク | システム > インターフェース**」から有効/無効にできるポートを示します。有効になっているポートは**有効** アイコン、無効になっているポートは**無効** アイコンで示されます。アイコンを選択すると、ポートを有効/無効にするかどうかを確認するメッセージが表示されます。「**OK**」を選択します。ポートが有効/無効になり、アイコンが変化します。
- **コメント** — ユーザ定義のコメント。
- **設定** — **編集**アイコンを選択するとダイアログが表示され、指定したインターフェースの設定を行うことができます。インターフェースの設定については、「インターフェースの設定」を参照してください。

仮想インターフェースの追加

トピック:

- 仮想インターフェースの一般設定
- 仮想インターフェースの詳細設定
- 仮想インターフェース（VLAN サブインターフェース）

インターフェースの概要については、次を参照してください。「物理インターフェースと仮想インターフェース」.

静的とは、固定 IP アドレスがインターフェースに割り当てられていることを意味します。

静的インターフェースを設定するには、以下の手順を実行します。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 「**インターフェース設定**」テーブルで、「**+ インターフェースの追加**」を選択し、設定するインターフェースの種別を選択します。オプションは、どのインターフェースを選択するかによって変化します。「**インターフェースの追加**」ダイアログが表示されます。

仮想インターフェースの一般設定

仮想インターフェースの一般設定を行うには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース|一般**」に移動します。
2. 「ゾーン」で、インターフェースに割り当てるゾーンを選択します。
   - **LAN**
   - **WAN**
   - **DMZ**
   - **WLAN**
   - ユーザが作成したユーザ定義ゾーン
   - 「**ゾーンの作成**」。「**ゾーンの追加**」ダイアログが表示されます。ゾーンの追加方法については、「*ゾーンについて*」を参照してください。

   ⓘ | **補足:** 表示されるオプションは、選択するゾーンによって変化します。
3. **ネットワーク モード**:で、次のように選択します。
   - **静的** (WAN での既定)
   - **静的 IP モード** (LAN での既定)
4. 「**IP アドレス**」フィールドと「**サブネット マスク**」フィールドに、インターフェースの IP アドレスとサブネット マスクを入力します。

ⓘ **補足:** 別のゾーンと同じサブネットにある IP アドレスは入力できません。

5. 設定対象によって、次の操作を行います。

   - WAN ゾーンのインターフェースまたは管理インターフェースを設定する場合は、ゲートウェイ装置の IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。

     ⓘ **補足:** WAN サブネットの IP アドレス空間に属さない WAN インターフェース経由で送信先に到達する必要がある場合は、WAN サブネット上のピア装置のルーティング プロトコルから既定のルートを動的に受信しているかどうかにかかわらず、WAN インターフェースにデフォルト ゲートウェイの IP アドレスを指定する必要があります。LAN インターフェースではデフォルト ゲートウェイ IP がオプションになっています。

   - LAN ゾーンのインターフェースまたは DMZ ゾーンのインターフェースを設定する場合は、ゲートウェイ装置の IP アドレスを「**デフォルト ゲートウェイ (オプション)**」フィールドに入力します。

   このインターフェースが内部ネットワークかプライベート ネットワークかにかかわらず、ゲートウェイ装置によって外部ネットワークへのアクセスが可能になります。

6. 設定対象によって、次の操作を行います。

   - LAN ゾーンのインターフェースを設定する場合は、「」に進みます。仮想インターフェースの一般設定
   - WAN ゾーンのインターフェースを設定する場合は、DNS サーバの IP アドレスを最大 3 つまで「**DNS サーバ**」フィールドに入力します。DNS サーバはパブリックでもプライベートでもかまいません。詳細については、「*WAN インターフェースの設定*」を参照してください。

7. 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース設定**」テーブルの「**コメント**」列に表示されます。
8. このインターフェースを介したセキュリティ装置のリモート管理を有効にするには、サポートされている**管理**プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、「**HTTP**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が淡色表示 (無効) になります。

   ⓘ **補足:** この機能の構成要素は、内部の「ユーザ認証の設定」オプションで制御することができます。詳細については、以下を参照してください。DP のオフロードによる HTTP/HTTPS リダイレクト.

   ⓘ **補足:** 同じセキュリティ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。

9. 限定的な管理権限を持つ選ばれたユーザがセキュリティ装置にログインすることを許可するには、「ユーザ ログイン」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、「**HTTP**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が淡色表示 (無効) になります。
10. **詳細設定**を行うには、「*静的インターフェースの詳細設定*」に進みます。
11. 「**OK**」を選択します。

    ⓘ **補足:** セキュリティ装置のアドレスを変更した後に暗号キーを再生成するには、管理者パスワードが必要です。

仮想インターフェースの詳細設定

静的インターフェースの詳細設定を行うには、以下の手順に従います。

1. 「**インターフェースの追加/編集**」ダイアログで、「**詳細**」を選択します。

ⓘ **補足:** 仮想インターフェースの「**詳細**」で利用可能なオプションは、選択したゾーンとプラットフォームによって異なります。

2. 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。イーサネット速度と通信方式を強制的に設定する場合は、「**リンク速度**」から以下のオプションの 1 つを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps — 全二重	10 Gbps – 全二重
100Mbps — 全二重	
100 Mbps — 半二重	
10 Mbps — 全二重	
10 Mbps — 半二重	

△ **注意: 特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードから セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。**

3. 「**既定の MAC アドレスを使用する**」が既定で選択されています。インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**設定した MAC アドレスへ書き換える**」を選択し、フィールドに MAC アドレスを入力します。

4. 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。このオプションは、既定では選択されていません。
このオプションを無効にすると、インターフェースが有効になり、リンクは稼働状態に戻ることができます。

   ⓘ **重要:** 管理インターフェースや現在使用中のインターフェースは停止できません。
   このオプションを選択すると、確認メッセージが表示されます。「**OK**」を選択してポートを停止します。

   ⓘ **ヒント:** インターフェースを停止するには、インターフェースの「**有効**」列の「**有効**」アイコンを選択します。確認メッセージが表示されます。
   - 「**OK**」を選択すると、「**有効**」アイコンが「**無効**」アイコンに変わります。インターフェースを有効にするには、「**無効**」アイコンを選択します。確認メッセージが表示されます。
   - 「**OK**」を選択すると、「**無効**」アイコンが「**有効**」アイコンに変わります。

5. AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。
6. 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。
7. 必要に応じて、「**既定 802.1p CoS を有効にする**」を選択して、このインターフェースを通過する情報に QoS（サービス品質）管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

   ⓘ **補足:** このオプションは、VLAN インターフェースでのみ利用できます。

   このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**ポリシー | ルールとポリシー > アクセス ルール**」にあるアクセス ルールで制御されます。
8. 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。
9. 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。
10. 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが LAN、DMZ、または WLAN インターフェースに対して表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。
11. 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの非対称ルートのサポートを有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。
12. 次の各ケースで TZ シリーズ セキュリティ装置を設定する場合
    - LAN/DMZ/WLAN インターフェースでは、「*ルート モードの設定*」に進みます。
    - WAN インターフェースでは、ステップ 15 に進みます。
13. 必要に応じて、「**冗長/統合ポート**」から「**リンク統合**」または「**ポート冗長化**」を選択します。詳細については、「*リンク統合とポート冗長化の設定*」を参照してください。

14. WAN インターフェースが断片化せずに転送できる最大パケット サイズ（MTU – 最大転送単位）を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット（既定）	1500
ジャンボ フレーム パケット	9000

ⓘ **補足:** ポートでジャンボ フレームを処理するには、「*ポリシー管理*」の説明に従って、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

15. 必要に応じて、このインターフェースの MTU 値よりも大きな VPN 以外の送信パケットを断片化するには、「VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものを断片化する」を選択します。このオプションは、既定では選択されています。選択すると、以下のオプションが利用可能になります。

ⓘ **重要:** 発信 VPN トラフィックの断片化の指定は、「**詳細設定**」で行います。

16. 必要に応じて、Do-not-fragment packet（パケットの断片化を行わない）ビットをオーバーライドするには、「**DF (Don't Fragment: 断片化を行わない) ビットを無視する**」を選択します。このオプションは、既定では選択されていません。
17. WAN インターフェースが断片化されたパケットを受信できるという通知を遮断するには、「**インターフェースの MTU より大きい送信パケットに対して ICMP 要断片化を送信しない**」を選択します。このオプションは、既定では選択されていません。
18. このインターフェースで帯域幅管理を設定するには、「**インターフェースでの帯域幅管理の有効化**」に進みます。
19. 「**OK**」を選択します。

仮想インターフェース (VLAN サブインターフェース)

VLAN サブインターフェースを追加する場合は、それをゾーンに割り当て、VLAN タグを割り当てて、さらに物理インターフェースに割り当てる必要があります。ゾーンの割り当てに基づき、同じゾーンの物理インターフェースを設定するときと同じように VLAN サブインターフェースを設定します。

仮想インターフェースを追加するには、次の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 「**インターフェース設定**」で、「**+ インターフェースの追加**」から「**仮想インターフェース**」を選択します。「**仮想インターフェースの追加**」ダイアログが表示されます。

3. インターフェースに割り当てる**ゾーン**を選択します。LAN、WAN、DMZ、または WLAN を選択するか、新しいゾーンを作成できます。ゾーンの割り当ては、必ずしも親（物理）インターフェースと合わせる必要はありません。実際、親インターフェースを**未定義**のままにすることも可能です。

   サブインターフェースのネットワーク設定で何を選択するかは、選択したゾーンによって異なります。

   - **LAN**、**DMZ**、または保護種別の**新しいゾーンの作成** ― **静的**または**トランスペアレント**
   - **WLAN** または個別無線ゾーン ― 静的 IP のみ（モードはリストされない）

4. 「**VLAN タグ**」フィールドで、VLAN タグ（ID）をサブインターフェースに割り当てます。有効な VLAN ID は **0**（既定値）～ 4094 です。ただし、一部のスイッチでは、VLAN 1 がネイティブ VLAN 指定用に予約され、VLAN 0 が QoS 用に予約されています。お使いの装置で保護したい VLAN ごとに、対応する VLAN ID を持つ VLAN サブインターフェースを作成する必要があります。

   ⓘ **重要：**X シリーズ スイッチがプロビジョニングされている場合、0 ～ 35 の VLAN ID は内部 VLAN ID であり、VLAN サブインターフェースには使用できません。

5. このサブインターフェースが属することになる親（物理）インターフェースを「**親インターフェース**」で選択します。1 つのインターフェースに対して割り当てることのできるサブインターフェース数に制限はありません。サブインターフェースはシステムの上限に達するまでいくつでも割り当てることができます。
6. 選択したゾーンに基づき、サブインターフェースのネットワーク設定を行います。以下のインターフェース設定手順を参照してください。

   - 静的インターフェースの設定
   - 静的インターフェースの詳細設定
   - インターフェースのトランスペアレント IP モード（L3 サブネットを結合）の設定
   - 無線インターフェースの設定
   - WAN インターフェースの設定

7. サブインターフェースの管理方法とユーザのログイン方法を選択します。
8. 「**OK**」を選択します。

4to6トンネル インターフェースの追 加

このテキストを削除して独自のコンテンツで置き換えてください。

詳 細

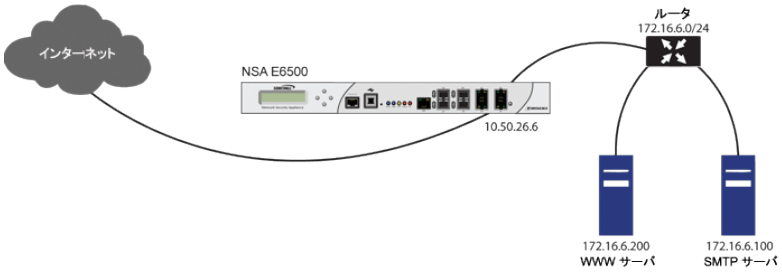
このテキストを削除して独自のコンテンツで置き換えてください。

ルート モードの設 定

ルート モードは、別々のパブリック IP アドレス範囲の間でトラフィックをルーティングするための NATの代替策を提供します。「*ルート モードの設定*」のトポロジについて考えます。セキュリティ装置が 2 つのパブリック IP アドレス範囲の間でトラフィックをルーティングしています。

- 10.50.26.0/24
- 172.16.6.0/24

ルート モードの設定



172.16.6.0 用のインターフェースでルート モードを有効にすることにより、そのインターフェースの NAT 変換は自動的に無効になり、10.50.26.0 用に設定された WAN インターフェースにすべての送受信トラフィックがルーティングされるようになります。

ⓘ **補足:** ルート モードは、LAN、DMZ、および WLAN のゾーンのインターフェースに静的 IP モードを使用する場合に利用できます。DMZ の場合は、レイヤ 2 ブリッジ モードを使用する場合も利用できます。ルート モードは WAN モードでは使用できません。

ルート モードを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 適切なインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**詳細**」を選択します。
4. 「**エキスパート モード設定**」セクションまでスクロールします。

5. インターフェースでルート モードが有効にするには、「**ルート モードを使用する – 発信/受信の変換を防ぐための NAT ポリシーを追加します**」を選択します。このオプションは、既定では選択されていません。これを選択すると、次の**エキスパート モード**設定が使用できるようになります。
6. 「**NAT ポリシー発信/受信インターフェース**」から、そのインターフェースのトラフィックをルーティングするために使用する WAN インターフェースを選択します。既定は「**すべて**」です。
7. 断片化せずに転送できる最大パケット サイズ (MTU – 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

ⓘ **補足:** ポートでジャンボ フレームを処理するには、あらかじめジャンボ フレームのサポートを有効にしておく必要があります。ジャンボ フレーム パケットのバッファ サイズの要件により、ジャンボ フレームをサポートするためのメモリ要件は 4 倍になります。

装置で帯域幅管理が有効になっている場合は、「帯域幅管理」セクションが表示されます。このインターフェースで帯域幅管理を設定するには、「*インターフェースでの帯域幅管理の有効化*」に進みます。

8. 「**OK**」を選択します。

ⓘ **重要:** 装置は、設定されたインターフェースと選択された WAN インターフェースの両方について「NAT ではない」ポリシーを作成します。これらのポリシーは、より一般的なM21 NAT ポリシーが設定されていても、それらに優先して使用されます。

インターフェースでの帯域幅管理の有効化

帯域幅管理 (BWM) により、最小帯域幅の保証と、トラフィックの優先順位付けが可能になります。帯域幅管理は、**「ファイアウォール設定 > 帯域幅管理」**で有効にします。アプリケーションやユーザの帯域幅の量を制御することにより、利用可能な帯域幅すべてを少数のアプリケーションやユーザが消費することを防げます。異なるネットワークトラフィックに割り当てられた帯域幅のバランスをとり、そしてトラフィックに優先順位を付けることで、ネットワークのパフォーマンスを向上できます。

さまざまな種別の帯域幅管理を有効にできます。

- **詳細** – 帯域幅オブジェクト、アクセス ルール、そしてアプリケーション ポリシーを設定することにより、インターフェース毎に送信および受信の最大帯域幅制限を設定できます。
- **グローバル** – 帯域幅管理設定をグローバルに有効にして、それらをすべてのインターフェースに適用できます。
- **Global Enh (拡張グローバル)** – 「グローバル」に似ていますが、先着順のキューを使用し、処理するパケット数を制限しません。
- **なし** – (既定) 帯域幅管理は無効です。

帯域幅管理の設定と各種帯域幅管理の効果については、https://www.sonicwall.com/ja-jp/support/technical-documentation/ にある SonicOS 管理マニュアルを参照してください。

SonicOS では、すべてのインターフェース上の送信 (発信) トラフィックと受信 (着信) トラフィックの両方に帯域幅管理を適用できます。送信帯域幅管理は、等級ベース キューイングを使用して行われます。受信帯域幅管理は、TCP 固有の動作を使用してトラフィックを制御する、ACK 遅延アルゴリズムを実装することによって行われます。

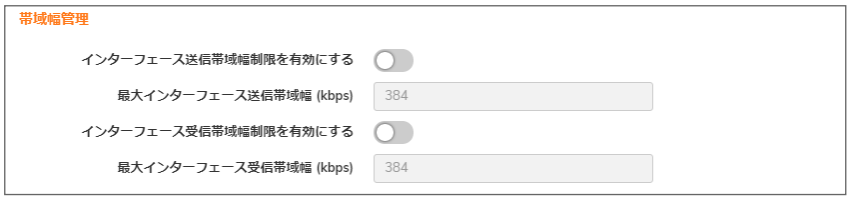
等級ベース キューイング (CBQ) により、ファイアウォールの保証された帯域幅と最大帯域幅のサービス品質 (QoS) が提供されます。そのインターフェース宛てのすべてのパケットは、対応する優先順位のキューに登録されます。スケジューラは、パケットのキュー登録を解除して、フローの保証された帯域幅と利用可能なリンクの帯域幅に応じて、パケットをリンク上で送信します。

このセクションで説明するオプションは、帯域幅管理が**「ファイアウォール設定 > 帯域幅管理」**で有効になっている場合にのみ使用可能です。

受信および送信の帯域幅管理を有効または無効にするには、以下の手順を実行します。

1. **「ネットワーク | システム > インターフェース」**に移動します。
2. インターフェースの**編集**アイコンを選択します。**「インターフェースの編集」**ダイアログが表示されます。
3. 未定義のインターフェースの場合は、「インターフェースの設定」に記載の各セクションに従ってインターフェースを設定します。

4. 「**詳細**」画面で「**帯域幅管理**」までスクロールします。



ⓘ **補足:** 「**詳細設定**」は、セキュリティ装置のモデルや選択したゾーンの種別によって異なる場合があります。

5. このインターフェースでの**帯域幅管理**を有効にします。

   a. 送信トラフィックをインターフェースの最大帯域幅に制限するには、「**送信帯域幅制限を有効にする**」を選択します。このオプションは、既定では選択されていません。

   最大帯域幅を「**最大インターフェース送信帯域幅 (kbps)**」フィールドに指定します。最小値は 20 Kbps、最大値は 1000000、既定値は 384.000000 です。

   b. 受信トラフィックをインターフェースの最大帯域幅に制限するには、「**受信帯域幅制限を有効にする**」を選択します。このオプションは、既定では選択されていません。

   最大帯域幅を「**最大インターフェース受信帯域幅 (kbps)**」フィールドに指定します。最小値は 20 Kbps、最大値は 1000000、既定値は 384.000000 です。

   これらのオプションのどちらかが選択されているかどうかで、次の違いが生じます。

   - 選択されている場合、利用可能な最大送信帯域幅管理は定義されていますが、詳細帯域幅管理はポリシー ベースなので、その制限は対応するアクセス ルールまたはアプリケーション ルールが存在しなければ適用されません。
   - 選択されていない場合は、帯域幅の制限はインターフェース レベルでは設定されませんが、トラフィックはその他のオプションを使用して調整できます。

6. 必要に応じて、「**既定 802.1p タグ付けを有効にする**」を選択して、このインターフェースを通過する情報に QoS (サービス品質) 管理のための 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

   このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**ポリシー | ルールとポリシー > アクセス ルール**」で設定したアクセス ルールで制御されます。

7. 「**OK**」を選択します。

インターフェースのトランスペアレント IP モード (L3 サブネットを結合) の設定

トピック:

- トランスペアレント IP モード インターフェースの詳細設定

トランスペアレント IP モードを有効にすると、装置は、WAN サブネットを内部インターフェースにブリッジできるようになります。

インターフェースをトランスペアレント モード用に設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 設定する「**未定義**」インターフェースの**設定**アイコンを選択します。「**インターフェースの設定**」ダイアログが表示されます。
3. 次のどちらかを行います。
   - 「**ゾーン**」で「**LAN**」または「**DMZ**」を選択します。
     ⓘ | **補足:** 利用可能なオプションは、選択するゾーンの種別によって異なります。
   - 設定可能なインターフェース用の新しいゾーンを作成する場合は、「**ゾーンの作成**」を選択します。「**ゾーンの追加**」ダイアログが表示されます。ゾーンの追加方法については、「*ゾーンについて*」を参照してください。
4. 「モード / IP 割り当て」から「トランスペアレント IP モード (L3 サブネットを結合)」を選択します。オプションが次のように変化します。
5. 「トランスペアレント範囲」で、このインターフェースを通じてアクセスする IP アドレスの範囲を含むアドレス オブジェクトを選択します。アドレス範囲は、LAN、DMZ、または、内部のトランスペアレント インターフェースに使用されるゾーンに一致するその他の保護ゾーンといった、内部ゾーン内にあることが必要です。

   要求を満たすアドレス オブジェクトが設定されていない場合は、「**アドレス オブジェクトの作成**」を選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。
6. 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース**」テーブルの「**コメント**」列に表示されます。このオプションは、既定では選択されていません。
7. このインターフェースを介した セキュリティ装置のリモート管理を有効にするには、サポートされている管理プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。このオプションは、既定では選択されていません。

   同じセキュリティ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。
8. 制限付き管理権限を持つ選ばれたユーザがこのインターフェースを使ってセキュリティ装置に直接ログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。
9. 「**管理**」や「**ユーザ ログイン**」のプロトコルに「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、選択されます。HTTP から HTTPS へのリダイレクトを防ぐには、このオプションの選択を解除します。

   ⓘ | **ヒント:** 「**ユーザ ログイン**」プロトコルで「**HTTP**」を選択すると、リダイレクトは無効になります。

   ⓘ | **補足:** この機能の構成要素は、内部の「**ユーザ認証の設定**」オプションで制御することができます。詳細については、「*DP のオフロードによる HTTP/HTTPS リダイレクト*」を参照してください。
10. 「**OK**」を選択します。

ⓘ | **補足:** 装置のアドレスを変更した後に暗号キーを再生成するには、管理者パスワードが必要です。

トランスペアレント IP モード インターフェースの詳細設定

トランスペアレント IP モード インターフェースの詳細設定を行うには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 変更するインターフェースの「**編集**」を選択します。
3. 「**インターフェースの編集**」ダイアログで、「**詳細**」を選択します。

4. 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。イーサネット速度と通信方式を強制的に設定する場合は、「**リンク速度**」から以下のオプションの 1 つを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps ー 全二重	10 Gbps – 全二重
100Mbps ー 全二重	
100 Mbps ー 半二重	
10 Mbps ー 全二重	
10 Mbps ー 半二重	

△ **注意: 特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードから セキュリティ装置への接続の速度と通信方式も強制的に変更する必要があります。**

5. 「**既定の MAC アドレスを使用する**」が既定で選択されています。インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**既定の MAC アドレスを上書きする**」を選択し、フィールドに MAC アドレスを入力します。
6. 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。このオプションは、既定では選択されていません。

   このオプションを無効にすると、インターフェースが有効になり、リンクは稼働状態に戻ることができます。このオプションは、既定では選択されていません。

   ⓘ **補足:** 管理インターフェースや現在使用中のインターフェースは停止できません。このオプションを選択すると、確認メッセージが表示されます。「**OK**」を選択してポートを停止します。

   ⓘ **ヒント:** インターフェースを停止するには、インターフェースの「**有効**」列の「**有効**」を選択します。確認メッセージが表示されます。
   - 「**OK**」を選択すると、「**有効**」アイコンが「**無効**」アイコンに変わります。インターフェースを有効にするには、「**無効**」アイコンを選択します。確認メッセージが表示されます。
   - 「**OK**」を選択すると、「**無効**」アイコンが「**有効**」アイコンに変わります。
7. AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。

8. 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。
9. 必要に応じて、「**既定 802.1p CoS を有効にする**」を選択して、このインターフェースを通過する情報に QoS（サービス品質）管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

   ⓘ | **補足:** このオプションは、VLAN インターフェースでのみ利用できます。

   このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**ポリシー | ルールとポリシー > アクセス ルール**」にあるアクセス ルールで制御されます。
10. 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。
11. 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。

    ⓘ | **補足:** TZ シリーズ装置だけに、このオプションがあります。
12. 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。
13. 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの**非対称ルートのサポート**を有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「*クラスタ設定における非対称ルーティング*」を参照してください。
14. 断片化せずに転送できる最大パケット サイズ（MTU – 最大転送単位）を指定するには、ポートが送受信するパケットのサイズを「**インターフェース MTU**」フィールドに入力します。

標準パケット（既定）	1500
ジャンボ フレーム パケット	9000

15. 帯域幅管理が有効になっている場合、このインターフェースで帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化」に進みます。
16. 「OK」を選択します。

無線インターフェースの設定

トピック:

- 無線インターフェースの詳細設定

無線インターフェースは無線ゾーンに割り当てられたインターフェースであり、SonicWall SonicWave の安全なアクセス ポイントをサポートするために使用されます。

SonicPoint は、セキュリティ種別の無線（既定では WLAN）のインターフェースでのみプロビジョニングと管理を行うことができます。

無線インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3. 「**ゾーン**」で、「**WLAN**」または定義済みの個別無線ゾーンを選択します。
4. 「**モード / IP 割り当て**」で、次のいずれかを選択します。
   - **静的 IP モード (既定)**。ステップ 12 に進みます。
   - **レイヤ 2 ブリッジ モード**
5. 「**OK**」を選択します。オプションが次のように変化します。

6. 「**ブリッジ先**」から、ブリッジする先のインターフェースを選択します。このインターフェースのブリッジ先として指定できるインターフェースだけが表示されます。
7. すべての非 IP トラフィックを遮断するには、「**すべての非 IP トラフィックを遮断する**」を選択します。
8. ブリッジ ペアでトラフィックをルーティングしないようにするには、「**このブリッジ ペアにトラフィックをルーティングしない**」を選択します。

9. 「**コメント**」フィールドに、必要に応じてコメント テキストを入力します。このテキストは、「**インターフェース**」テーブルの「**コメント**」列に表示されます。
10. このインターフェースを介したファイアウォールのリモート管理を有効にするには、サポートされている**管理**プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。
11. 限定的な管理権限を持つ特定のユーザが装置にログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。
12. 「管理」または「**ユーザ ログイン**」プロトコルで「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が使用可能になり、選択されます。「**ユーザログイン**」に対して「**HTTP**」を選択すると、「**HTTPS**」オプションは選択されていても選択が解除されます。
13. 「**OK**」を選択します。

無線インターフェースの詳細設定

無線インターフェースの詳細設定を行うには、以下の手順に従います。

1. 「**インターフェースの編集**」ダイアログで、「**詳細**」を選択します。表示されるオプションは、装置のプラットフォームによって異なります。

2. AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。このオプションは、既定では選択されています。
3. 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。このオプションは、既定では選択されていません。
4. 必要に応じて、「**既定 802.1p CoS を有効にする**」を選択して、このインターフェースを通過する情報に QoS（サービス品質）管理の 802.1p 優先順位情報のタグを付けます。このオプションは、既定では選択されていません。

   ⓘ | **補足:** このオプションは、VLAN インターフェースでのみ利用できます。

   このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**ポリシー | ルールとポリシー > アクセス ルール**」にあるアクセス ルールで制御されます。
5. 必要に応じて、インターフェースをルート通知から除外するには、「**ルート通知 (NSM, OSPF, BGP, RIP) から除外する**」を選択します。このオプションは、既定では選択されていません。

6. 必要に応じて、「**管理トラフィックのみ**」を選択し、トラフィックを SonicWall 管理トラフィックとルーティング プロトコルのみに制限します。このオプションは、既定では選択されていません。
7. 必要に応じて、DNS プロキシを有効にしている場合は「**DNS プロキシを有効にする**」オプションが表示されます。インターフェースで DNS プロキシを有効にするには、このオプションを選択します。このオプションは、既定では選択されていません。
8. 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、インターフェースでの非対称ルートのサポートを有効にします。有効にすると、このインターフェースから初期化されたトラフィックは非対称ルートをサポートします。つまり、初期パケットや応答パケットが他のインターフェースから通過できるようになります。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「*クラスタ設定における非対称ルーティング*」を参照してください。
9. 「**WAN に向けての重複回避用 ARP の転送を有効にする**」を選択すると、このインターフェースで受信した重複回避用 ARP パケットは、WAN インターフェースのハードウェア MAC アドレスを送信元 MAC アドレスとして、WAN に転送されます。
10. 「**WAN に向けての重複回避用 ARP 自動生成を有効にする**」を選択すると、このインターフェース上の新しいマシンの登録が ARP テーブルに追加されるたびに自動的に重複回避用 ARP パケットが WAN に送信されます。WAN インターフェースのハードウェア MAC アドレスが ARP パケットの送信元 MAC アドレスとして使用されます。
11. 断片化せずに転送できる最大パケット サイズ (MTU – 最大転送単位) を指定するには、ポートが送受信するパケットのサイズを「インターフェース MTU」フィールドに入力します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

12. このインターフェースでルート モードを設定する場合は、「ルート モードの設定」に進みます。
13. 帯域幅管理が有効になっている場合、このインターフェースで帯域幅管理を設定するには、「インターフェースでの帯域幅管理の有効化」に進みます。
14. 「OK」を選択します。

WAN インターフェースの設定

トピック:

- WAN インターフェースの詳細設定
- WAN インターフェースのプロトコルの設定

ⓘ **補足:** WAN サブネットの IP アドレス空間に属さない送信先に、WAN インターフェース経由で到達する必要がある場合は、WAN サブネット上の対向の装置のルーティング プロトコルから既定のルートを動的に受信しているかどうかにかかわらず、WAN インターフェースにデフォルト ゲートウェイの IP アドレスを指定する必要があります。

WAN インターフェースを設定することにより、インターネット接続が可能になります。装置には、最大で *N – 2* 個の WAN インターフェースを設定できます。ここで、*N* は装置で定義されたインターフェース (物理および VLAN インターフェース) の数です。ただし、X0 および MGMT インターフェースだけは WAN インターフェースとして設定できません。

WAN インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 未定義インターフェースを設定している場合は、「ゾーン」メニューから「**WAN**」を選択します。**既定の WAN** インターフェースを選択した場合は、「**ゾーン**」メニューで「**WAN**」が既に選択されています。
4. 「**ネットワーク モード**」から、以下のいずれかの WAN ネットワーク アドレッシング モードを選択します。

   ⓘ **補足:** 「ネットワーク モード」ドロップダウン メニューで選択するオプションによって、利用できるオプションが変わります。オプションを選択すると表示される各フィールドに、必要な情報を入力してください。

   - **静的** – 静的 IP アドレスを使うネットワーク用に装置を設定します。
   - **DHCP** – インターネット上の DHCP サーバから IP 設定を要求するように装置を設定します。「DHCP クライアントでの NAT」は、ケーブルおよび DSL ユーザ向けの一般的なネットワーク アドレス指定モードです。
   - **PPPoE** – PPPoE (Point to Point over Ethernet) を使用して、インターネットに接続します。ISP への接続にユーザ名とパスワードが必要な場合は、「**ユーザ名**」および「**ユーザ パスワード**」フィールドに入力します。DSL モデムを使用する場合は、このプロトコルが一般的です。
   - **PPTP** – PPTP (Point to Point Tunneling Protocol) を使用して、リモート サーバに接続します。トンネル接続が必要な旧式のマイクロソフト Windows実装をサポートします。
   - **L2TP** – IPsec を使用して L2TP (Layer 2 Tunneling Protocol) サーバに接続し、クライアントからサーバに送信されるすべてのデータを暗号化します。ただし、他の宛先へのネットワークトラフィックは暗号化しません。
   - **ワイヤ モード (2 ポート ワイヤ)** – バイパス、検査、保護の各モードで装置をネットワークに配備できます。詳細については、「*ワイヤ モードとタップ モードの設定*」を参照してください。
   - **タップ モード (1 ポート タップ)** – 装置をネットワークに配備し、ネットワーク タップ、ポート ミラーリング、SPAN ポートを使用できます。詳細については、「*ワイヤ モードとタップ モードの設定*」を参照してください。
5. **DHCP** を使用する場合は、必要に応じて「**ホスト名**」フィールドにわかりやすい名前を入力し、「**コメント**」フィールドに必要なコメントを入力します。
6. **PPPoE**、**PPTP**、**L2TP** を使用する場合は、次のようなフィールドが追加で表示されます。
   - 「**スケジュール**」が表示される場合は、このインターフェースで接続する時間のスケジュールをドロップダウン メニューから選択します。
   - 「**ユーザ名**」および「**ユーザ パスワード**」には、ISP から受領したアカウント名とパスワードを入力します。
   - 「**サーバ IP アドレス**」フィールドが表示される場合は、ISP から受領したサーバ IP アドレスを入力します。
   - 「**(クライアント) ホスト名**」フィールドが表示される場合は、装置のホスト名を入力します。これは、「**システム > 管理 | ファイアウォール管理者**」に表示されるファイアウォール名です。
   - 「**共有鍵**」フィールドが表示される場合は、ISP から受領した値を入力します。
7. このインターフェースを介した装置のリモート管理を有効にするには、サポートされている管理プロトコルを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。

   同じ装置の別のゾーンからの管理用 WAN インターフェースへのアクセスを許可するには、アクセス ルールを作成する必要があります。アクセス ルールの作成については、『*SonicOS ポリシー管理ガイド*』を参照してください。

8. PPPoE、PPTP、L2TP を使用する場合は、次のようなフィールドが追加で表示されます。
    - PPPoE の場合は、以下のいずれかを選択します。
        - PPPoE サーバから IP アドレスを取得するには、「**自動的に IP アドレスを取得する**」を選択します。
        - このインターフェースに静的 IP アドレスを使用する場合は、「**IP アドレスを指定する**」を選択し、IP アドレスをフィールドに入力します。
        - 「**アンナンバード インターフェース**」を選択し、次のいずれかを行います。
            - アンナンバード インターフェースを選択します。
            - 「**新規アンナンバード インターフェースの作成**」を選択して、新しいアンナンバード インターフェースを作成します。

        ⓘ | **補足:** このインターフェースは未割り当てでなければなりません。
    - PPTP または L2TP の場合は、次のオプションを設定します。
        - 「**ネットワーク モード**」で、次のいずれかを選択します。
            - 「**DHCP**」の場合、IP アドレス、サブネット マスク、デフォルト ゲートウェイの各フィールドはサーバによって自動的に設定されます。
            - 「**静的**」の場合、これらのフィールドに適切な値を入力します。
        - 「**無動作時切断**」を選択し、時間（分）を入力すると、動作がない状態でこの時間が経過すると、接続が切断されます。無動作タイムアウトを無効にするには、このオプションを無効にします。
9. DHCP を使用する場合は、必要に応じて以下の選択を行います。
    - DHCP サーバから前回提供された IP アドレスと同じアドレスを WAN インターフェース用に要求する場合は、「**起動時に前の IP の更新を要求する**」を選択します。
    - この WAN インターフェースの切断後の再接続の際に毎回 DHCP サーバにリース再取得の要求を送信する場合は、「**リンク アップ時に DHCP リースを再取得する**」を選択します。

    次のオプションの下に表示されるフィールドは、DHCP サーバから割り当てられます。プロビジョニングの後、以下のボタンが使用可能になるので選択を行います。
    - 「**再取得**」を選択すると、現在割り当てられている IP アドレスの DHCP リース期間がリセットされます。
    - 「**破棄**」を選択すると、現在の IP アドレスの DHCP リースがキャンセルされます。接続は破棄されます。接続を再確立するには、DHCP サーバから新しい IP アドレスを取得する必要があります。
    - 「**再表示**」を選択すると、DHCP サーバから新しい IP アドレスを取得します。
10. 制限付き管理権限を持つ選ばれたユーザがこのインターフェースを使って装置に直接ログインすることを許可するには、「**ユーザ ログイン**」で、「**HTTP**」と「**HTTPS**」のいずれかまたは両方を選択します。
11. HTTP 接続を装置への安全な HTTPS 接続に自動的にリダイレクトするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「*HTTP/HTTPS リダイレクト*」を参照してください。
12. 「*WAN インターフェースの詳細設定*」の説明に従って、「**詳細**」タブおよび「**プロトコル**」タブ（表示される場合）で設定を続行します。
13. 詳細設定を行うには、「*WAN インターフェースの詳細設定*」に進みます。
14. 「**IP 割り当て**」で「**PPPoE**」、「**PPTP**」、または「**L2TP**」を選択した場合は、「*WAN インターフェースのプロトコルの設定*」に進みます。
15. 「**OK**」を選択します。

WAN インターフェースの詳細設定

WAN インターフェースの詳細設定を行うには、以下の手順に従います。

1. 「**インターフェースの編集**」ダイアログで、「**詳細**」を選択します。
2. 「**リンク速度**」では、「**自動ネゴシエーション**」が既定で選択され、接続された機器はイーサネット接続の速度と通信方式を自動的にネゴシエートします。強制的に変更したイーサネット速度と通信方式を指定する場合は、「**リンク速度**」メニューから以下のいずれかのオプションを選択します。

1 Gbps のインターフェースの場合	10 Gbps のインターフェースの場合
1Gbps ー 全二重	10 Gbps – 全二重
100Mbps ー 全二重	
100 Mbps ー 半二重	
10 Mbps ー 全二重	
10 Mbps ー 半二重	

ⓘ **重要:** 特定のイーサネット速度と通信方式を選択した場合は、イーサネット カードからファイアウォールへの接続の速度と通信方式も強制的に変更する必要があります。

3. インターフェースの「**既定の MAC アドレスを使用する**」をオーバーライドするには、「**設定した MAC アドレスへ書き換える**」を選択し、フィールドに MAC アドレスを入力します。
4. 保守またはその他の理由でこのインターフェースを一時的にオフラインにする場合は、「**ポートを停止する**」を選択します。接続していたリンクは切断されます。チェックボックスをオフにすると、インターフェースが有効になり再びリンクが接続されます。
5. AppFlow 機能については、「**フロー報告を有効にする**」を選択すると、このインターフェースに対して作成されたフローのフロー報告が有効になります。
6. 「**マルチキャスト サポートを有効にする**」を選択して、このインターフェースでマルチキャスト受信を許可します。
7. このインターフェースを通過する情報に QoS (Quality of Service) 管理のための 802.1p 優先順位情報のタグを付けるには、「**802.1p タグ付けを有効にする**」を選択します。このインターフェースを通じて送信されるパケットは、VLAN id=0 のタグ付けが行われ、802.1p 優先順位情報を搬送します。この優先順位情報を利用するには、このインターフェースに接続されている機器が、優先順位フレームをサポートしている必要があります。QoS 管理は、「**オブジェクト | プロファイル オブジェクト > QoS 級割**」にあるアクセス ルールで制御されます。QoS および帯域幅管理の詳細については、『*SonicOS システム管理ガイド*』を参照してください。
8. 必要に応じて、「**冗長/統合ポート**」ドロップダウン リストから、「**リンク統合**またはポート冗長化」を選択します。詳細については、「*リンク統合とポート冗長化の設定*」を参照してください。
9. **インターフェース MTU** ー インターフェースが、パケットを断片化せずに転送できるパケットの最大サイズを指定します。ポートが送受信するパケットのサイズを特定します。

標準パケット (既定)	1500
ジャンボ フレーム パケット	9000

   - **VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものを断片化する** ー VPN 以外の送信パケットでこのインターフェースの MTU 値以上の大きさのものをすべて断片化することを指定します。VPN 送信パケットの断片化の指定は、「**ネットワーク |IPSec VPN | ポリシー/設定**」で設定します。VPN トラフィックの詳細については、『*SonicOS ネットワーク管理ガイド*』を参照してください。

- **DF (Don't Fragment: 断片化を行わない) ビットを無視する** — パケットの DF ビットをオーバーライドします。
- **ICMP の「フラグメント必要」メッセージを生成しない** — このインターフェースが断片化されたパケットを受信できるという通知を遮断します。

10. DHCP を使用する場合は、次のオプションが表示されます。
    - サーバが変わる可能性がある場合は、「**DHCP の使用時に「検出」を使って更新を開始する**」を選択します。
    - DHCP サーバがすぐに応答しない可能性がある場合は、「**リース取得中に _ 秒間隔で「DHCP 発見」を送信する**」を選択し、その間隔の秒数を調節します。
11. 必要に応じて、このインターフェースでの帯域幅管理を有効にします。帯域幅管理の詳細については、「インターフェースでの帯域幅管理の有効化」を参照してください。

WAN インターフェースのプロトコルの設定

WAN インターフェースの設定時に「**IP 割り当て**」で「**PPPoE**」、「**PPTP**」、または「**L2TP**」を指定した場合は、「**インターフェースの編集**」ダイアログに「**プロトコル**」ビューが表示されます。

「**プロトコル**」ビューの「**設定の取得先**」セクションのフィールド (**SonicWall の IP アドレス、サブネット マスク、ゲートウェイ アドレス**など) は、インターネット サービス プロバイダ (ISP) から割り当てられます。装置を ISP に接続すると、これらのフィールドに実際の値が表示されます。

また、PPPoE を指定すると、SonicOS によって「**詳細**」ビューの「**インターフェース MTU**」オプションが「**1492**」に設定され、「**プロトコル**」ビューのその他の設定も割り当てられます。

PPPoE のその他の設定を行うには、次の手順に従います。

1. 「**インターフェースの編集**」ダイアログで、「**プロトコル**」を選択します。
2. 「**PPPoE クライアント設定**」セクションの次のオプションを有効にします。
    - **無動作時に切断 (分)**: 時間を分で入力します (既定は 10 分)。パケットが送信されない状態でこの時間が経過すると、SonicOS は接続を切断します。このオプションは、既定では選択されていません。
    - **サーバ キープアライブに LCP Echo パケットを厳密に使用する**: PPPoE サーバから ppp LCP echo request パケットが 1 分間送信されていないことを検知したときに、SonicOS が接続を切断するようにするにはこれを選択します。このオプションは、PPPoE サーバが send LCP echo 機能をサポートする場合のみ選択してください。このオプションは、既定では選択されていません。
    - **サーバがトラフィックを送信しない場合、PPPOEクライアントを切断する – 分**: PPPoE サーバがパケット (LCP echo request を含む) を一切送信しないままその時間が経過したときに SonicOS によって接続が切断され、その後その再接続が行われることになる時間を分単位 (既定では **5** 分) を入力します。このオプションは、既定では選択されています。

トンネル インターフェースの設定

SonicOS では、次のようなさまざまな種別のトンネル インターフェースを設定できます。

- 番号付けされたトンネル インターフェースと番号付けされないトンネル インターフェース、WLAN トンネル インターフェース、IPv6 6to4 トンネル インターフェースは、「**ネットワーク | システム > インターフェース**」で設定します。

- ドロップ トンネル インターフェースと VPN トンネル インターフェースは、「**ネットワーク | システム > 動的ルーティング**」から設定します。詳細については、「*ルート通知とルート ポリシーの設定*」を参照してください。
- 番号付けされていないトンネル インターフェースは、「**ネットワーク | IPSec VPN > ルールと設定**」から VPN ポリシーの一部として設定します。VPN ポリシーについては、『*SonicOS IPSec VPN 管理ガイド*』を参照してください。

番号付けされたトンネル インターフェースと番号付けされないトンネル インターフェースは、VPN で使用されます。番号付けされたトンネル インターフェースには固有の IP アドレスが割り当てられますが、番号付けされないトンネル インターフェースは、既存の物理または仮想 (VLAN) インターフェースから IP アドレスを借用します。

どちらの種別のインターフェースも静的ルーティングと RIP および OSPF による動的ルーティングをサポートしますが、番号付けされたトンネル インターフェースは BGP にも対応しています。

また、番号付けされた VPN と番号付けされないトンネル インターフェースの両方が高度なルーティングをサポートでき、番号付けされないしトンネル インターフェースには制限がありません。

各種トンネル インターフェースの設定については、以下のセクションを参照してください。

- 番号付けされたトンネル インターフェース – 「*VPN トンネル インターフェースの設定*」
- 番号付けされないトンネル インターフェース – 『*SonicOS ネットワーク管理ガイド*』
- WLAN トンネル インターフェース – 「*WLAN トンネル インターフェースの作成*」
- ドロップ トンネル インターフェース – 「*ドロップ トンネル インターフェース*」
- IPv6 6to4 トンネル インターフェース – 「*6to4 自動トンネルの設定*」

VPN トンネル インターフェースの設定

「**インターフェースの追加**」ドロップダウン メニューから「**VPN トンネル インターフェース**」を選択して、番号付けされたトンネル インターフェースを作成できます。VPN トンネル インターフェースは、インターフェース 設定テーブルに追加されると、RIP、OSPF、BGP などの動的ルーティングに使用できるようになります。また、静的ルート ベース VPN の設定において、静的ルート ポリシーのインターフェースとして使用できるようになります。

VPN トンネル インターフェース (TI) は標準インターフェースと同じように設定して、装置管理や HTTP/HTTPS/Ping/SSH によるユーザ ログインを有効にすることができます。また、マルチキャスト、フロー報告、非対称ルーティング、断片化パケットの処理、DF (Don't Fragment: 断片化を行わない) ビットも設定できます。

ⓘ **補足:** 同じ VPN ポリシーと番号付けされたトンネル インターフェースをリモート ゲートウェイにも設定する必要があります。これらの番号付けされたトンネル インターフェース (ローカル ゲートウェイとリモート ゲートウェイ) に割り当てる IP アドレスは同じサブネットにある必要があります。

「*VPN トンネル インターフェースの配備*」は、VPN トンネル インターフェースを配備する方法を示しています。

VPN トンネル インターフェースの配備

TI をインターフェースとして設定できる機能	TI を使用できないインターフェース
静的ルート	静的 ARP 登録インターフェース
NAT	HA インターフェース
ACL (仮想アクセス ポイント アクセス制御リスト)	WLB (WAN 負荷分散) インターフェース
	静的 NDP (近隣者検出プロトコル) 登録インターフェース
OSPF	OSPFv3/RIPnG: 現在は IPv6 の高度なルーティングでサポートされていない
RIP	MAC_IP アンチスプーフ インターフェース
BGP	DHCP サーバ インターフェース

すべてのプラットフォームで、サポートされる VPN トンネル インターフェース（番号付けされるトンネル インターフェース）の最大数は 64 です。番号付けされないトンネル インターフェースの最大数はプラットフォームによって異なり、各プラットフォームでサポートされる VPN ポリシーの最大数と一致します。

VPN トンネル インターフェースを設定するには、以下の手順を実行します。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 「**インターフェース設定**」テーブルの下の「**インターフェースの追加**」で、「**VPN トンネル インターフェース**」を選択します。「**トンネル インターフェースの追加**」ダイアログが表示されます。

ゾーンは VPN として定義されており、変更できません。

3. 「**VPN ポリシー**」で、VPN ポリシーを選択します。
4. 「**名前**」フィールドに、このインターフェースのわかりやすい名前を入力します。この名前に使用できる文字は英数字、ピリオド (.)、下線 (_) です。空白とハイフン (-) は使用できません。
5. 「**IP アドレス**」フィールドに IP アドレスを入力します。既定値は `0.0.0.0` ですが、明示的な IP アドレスを入力する必要があります。そうしないとエラー メッセージが表示されます。
6. 「**サブネット マスク**」フィールドに、サブネット マスクを入力します。既定値は `255.255.255.0` です。
7. 必要に応じて、「**コメント**」フィールドにコメントを入力します。
8. 必要に応じて、このインターフェースで許可される**管理**プロトコルを指定します。**HTTPS**、**Ping**、**SNMP**、**SSH** から 1 つ以上を選択できます。
9. 必要に応じて、このインターフェースで許可される**ユーザ ログイン** プロトコルを指定します。**HTTP** と **HTTPS** のどちらかまたは両方を選択できます。

10. 「**詳細**」を選択します。

11. トンネル インターフェースに対して作成されるフローのフロー報告を有効にするには、「**フロー報告を有効にする**」を選択します。
12. 必要に応じて、「**マルチキャスト サポートを有効にする**」を選択し、インターフェースでのマルチキャスト受信を有効にします。このオプションは、既定では選択されていません。
13. 必要に応じて、「**非対称ルートのサポートを有効にする**」を選択し、トンネル インターフェースでの非対称ルートのサポートを有効にします。このオプションは、既定では選択されていません。非対称ルーティングの詳細については、「*非対称ルーティング*」を参照してください。
14. ルート モードを使用して発信/着信の変換を防ぐための NAT ポリシーを追加するには、「**ルート モードを使用する - 発信/着信の変換を防ぐための NAT ポリシーを追加します**」を選択します。選択すると、以下のオプションが利用可能になります。このオプションは、既定では選択されていません。
15. 「**ルート モード**」が選択されている場合、NAT ポリシーのインターフェースを指定するには、「NAT ポリシー発信/着信インターフェース」でインターフェースを選択します。使用できるインターフェースは装置によって異なります。既定は「**すべて**」です。
16. このインターフェースで断片化パケットの処理を有効にするには、「**断片化パケットの処理を有効にする**」を選択します。このオプションがオフの場合、断片化パケットは破棄され、VPN ログ レポートにログ メッセージ「Fragmented IPsec packet dropped」(断片化された IPSec パケットが破棄された) が表示されます。

    このオプションをオンにすると、「**DF (断片化を行わない) ビットを無視する**」オプションが使用できるようになります。
17. パケット ヘッダーの DF ビットを無視するには、「**DF (Don't Fragment: 断片化を行わない) ビットを無視する**」を選択します。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**」オプションを明示的に設定できます。これにより、すべての装置にそのパケットを断片化しないよう指示されます。このオプションが有効になっていると、装置は DF ビットを無視し、パケットの断片化を強行します。
18. 「**OK**」を選択します。新しい番号付けされた VPN トンネル インターフェースが「**インターフェース設定**」テーブルに追加されます。

リンク統合とポート冗長化の設定

リンク統合もポート冗長化も、SonicOS 管理インターフェースの「**インターフェースの編集**」ダイアログの「**詳細**」ビューで設定します。

- **リンク統合** — 複数のイーサネット インターフェースをまとめて単一の論理リンクにし、それによって単一の物理インターフェースを上回るスループットをサポートします。そのため、2 つのイーサネット ドメイン間でマルチギガビットのトラフィックが送信できるようになります。
- **ポート冗長化** — 第 2 のスイッチに接続できる任意の物理インターフェースに対して単一の冗長ポートを設

定して、プライマリ インターフェースまたはプライマリ スイッチに障害が起きた場合に接続が失われるのを防ぎます。

トピック:

- リンク統合
- リンク統合の設定
- ポート冗長化
- ポート冗長化の設定

リンク統合

リンク統合は、ファイアウォールとスイッチの間で利用可能な帯域幅を増やすために使用され、最高で 4 つのインターフェースをまとめて 1 つの統合リンクにすることで行われます。これは LAG (Link Aggregation Group) と呼ばれます。統合リンクのすべてのポートは、同じスイッチに接続されていなければなりません。装置は、リンク統合グループ内のインターフェース間でのトラフィックの負荷分散のためにラウンドロビン アルゴリズムを使用します。リンク統合は一定の冗長化も提供します。つまり、LAG 内の 1 つのインターフェースがダウンしても、他のインターフェースの接続は維持されるということです。

リンク統合は、ベンダーによって呼称が異なり、ポート チャンネル、イーサ チャンネル、トランク、ポート グルーピングなどと呼ばれることもあります。

トピック:

- リンク統合フェイルオーバー
- リンク統合の制限
- リンク統合の設定

リンク統合フェイルオーバー

SonicWall は、リンク障害で接続が失われるのを防ぐために、高可用性 (HA)、負荷分散グループ (LB グループ)、リンク統合といった複数の方法を用意しています。装置上でこれらの機能が 3 つとも設定されている場合、リンク障害の際に次の優先順位が適用されます。

1. 高可用性
2. リンク統合
3. 負荷分散グループ

リンク統合よりも HA が優先されます。LAG 内の各リンクは負荷を平等に分担するので、アクティブ ファイアウォールのリンクが失われると、アイドル ファイアウォールへのフェイルオーバーが強制的に行われます (そのファイアウォールのすべてのリンクの接続が維持されている場合)。物理的な監視を設定する必要があるのは、プライマリ統合ポートについてだけです。

リンク統合と LB グループを併用すると、リンク統合が優先されます。LB が作動するのは、統合リンクのすべてのポートがダウンした場合だけです。

リンク統合の制限

- 現在、リンク統合では静的アドレッシングのみがサポートされています。PAG (ポート統合化) と呼ばれる静的ポート チャンネルは、イーサネット ポート チャンネルを設定する 1 つの方法です。パートナー機器 (スイッチやサーバなど) とのイーサチャンネルを形成するために送信される LACP パケットや PAGP パケットはありません。

- イーサネット ポート チャンネルを使用して設定される静的 LAG (Link Aggregation Group) は、NSA 3600 以降のセキュリティ装置では手動で設定/バンドルする必要があります。
- 現在、動的 LACP (Link Aggregation Control Protocol) はサポートされていません。IEEE LACP や Cisco の PAGP など、動的な、プロトコルを介したイーサーネット ポートのバンドルは、イーサネット ポート チャンネルを設定するもう 1 つの方法です。この方法では、LACP パケットや PAGP パケットがポートから送信されます。

リンク統合の設定

リンク統合を設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. リンク統合グループのマスターとして指定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**詳細**」を選択します。
4. 「**冗長/統合ポート**」で、「**リンク統合**」を選択します。その他のオプションが表示されます。
5. 装置上の現在割り当てられていないインターフェースごとに「**統合ポート**」オプションが表示されます。ポートはどれも選択されていません。LAG に割り当てる他のインターフェースを最高 3 つまで選択します。

   ⓘ **補足:** インターフェースを LAG に割り当てると、そのインターフェースの設定はリンク統合マスター インターフェースによって管理され、個別に設定することができなくなります。「**インターフェース設定**」テーブルには、そのインターフェースのゾーンが「**統合ポート**」として表示され、**設定**アイコンが表示されなくなります。
6. インターフェースの「**リンク速度**」を「**自動ネゴシエーション**」に設定します。
7. 「**OK**」を選択します。インターフェースでウェブ管理が設定されていない場合、メッセージが表示されます。
   a. 「**OK**」を選択します。
   b. 別のインターフェースで**ウェブ管理**を有効にします。

ⓘ **重要:** リンク統合には、スイッチ上に対応する設定が必要です。スイッチの負荷分散方法はベンダーによって異なります。リンク統合の設定については、スイッチのドキュメントを参照してください。リンク統合は、ポート チャンネル、イーサ チャンネル、トランク、ポート グルーピングなどと呼ばれることもあります。

ポート冗長化

ポート冗長化は、物理イーサネット ポートに対して冗長ポートを設定するための単純な方法です。これは単一障害点としてのスイッチの障害を防ぐのに役立つ機能であり、ハイエンドの配備では特にそうです。

プライマリ インターフェースがアクティブのとき、プライマリ インターフェースはそこを出入りするトラフィックをすべて処理します。プライマリ インターフェースがダウンすると、セカンダリ インターフェースが送受信トラフィックをすべて引き継ぎます。セカンダリ インターフェースはプライマリ インターフェースの MAC アドレスを引き継ぎ、フェイルオーバー イベントでの適切な重複回避用 ARP を送信します。プライマリ インターフェースが回復すると、プライマリ インターフェースはセカンダリ インターフェースからすべてのトラフィック処理の責務を再び引き継ぎます。

典型的なポート冗長化設定では、プライマリ インターフェースとセカンダリ インターフェースを別々のスイッチに接続します。これはプライマリ スイッチがダウンした場合のフェイルオーバー パスを提供します。両方のスイッチは同じイーサネット ドメインになければなりません。両方のインターフェースが同じスイッチに接続されている場合にもポート冗長化を設定することができます。

ポート冗長化フェイルオーバー

SonicWall は、リンク障害で接続が失われるのを防ぐために、高可用性 (HA)、負荷分散グループ (LB グループ)、ポート冗長化といった複数の方法を用意しています。装置上でこれらの機能が 3 つとも設定されている場合、リンク障害の際に次の優先順位が適用されます。

1. ポート冗長化
2. HA
3. LB グループ

ポート冗長化と HA を併用すると、ポート冗長化が優先されます。一般に、インターフェース フェイルオーバーは HA フェイルオーバーを発生させますが、そのインターフェースで冗長ポートが利用可能であれば、インターフェース フェイルオーバーが発生しても HA フェイルオーバーは発生しません。プライマリ ポートとセカンダリの冗長ポートが両方ともダウンした場合は、HA フェイルオーバーが発生します (ただし、セカンダリ セキュリティ装置の対応するポートがアクティブであると仮定します)。

ポート冗長化と LB グループを併用しても、やはりポート冗長化が優先されます。1 つのポート (プライマリまたはセカンダリ) の障害であれば、HA の場合と同様にポート冗長化で処理されます。両方のポートがダウンした場合は、LB が作動し、代替インターフェースを探します。

ポート冗長化の設定

ポート冗長化を設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. リンク統合グループのマスターとして指定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**詳細**」を選択します。
4. インターフェースの「**リンク速度**」を「**自動ネゴシエーション**」に設定します。
5. 「**冗長/統合ポート**」で、「**ポート冗長化**」を選択します。別のオプションが表示されます。
6. この「**冗長ポート**」オプションには、現在割り当てられていない利用可能なインターフェースがすべて表示されます。いずれかのインターフェースを選択します。既定では「**なし**」になっています。

   ⓘ **補足:** いずれかのインターフェースを冗長ポートとして選択すると、そのインターフェースの設定はプライマリ インターフェースによって管理され、個別に設定することができなくなります。「**インターフェース設定**」テーブルには、そのインターフェースのゾーンが「**冗長ポート**」として表示され、**設定**アイコンが表示されなくなります。
7. 「**OK**」を選択します。インターフェースでウェブ管理が設定されていない場合、メッセージが表示されます。
   a. 「**OK**」を選択します。
   b. 別のインターフェースで**ウェブ管理**を有効にします。

IPS スニッファ モードの装置の設定

装置を設定して IPS スニッファ モードを有効にするには、同じゾーンにある 2 つのインターフェースを L2 ブリッジ ペアに使用します。WAN インターフェース以外のインターフェースであれば、どれでも使用できます。この例では、X2 と X3 がブリッジ ペアに使用され、LAN ゾーン内で設定されています。WAN インターフェース (X1) は、必要に応じてセキュリティ装置データ センターにアクセスするためにセキュリティ装置で使用されます。スイッチ上のミラーリングされたポートは、ブリッジ ペアの一方のインターフェースに接続しています。

トピック:

IPS スニッファ モード用の設定タスク リスト

- プライマリ ブリッジ インターフェースの設定
  - プライマリ ブリッジ インターフェースの LAN ゾーンの選択
  - 静的IP アドレスの割り当て
- セカンダリ ブリッジ インターフェースの設定
  - セカンダリ ブリッジ インターフェースの LAN ゾーンの選択
  - プライマリ ブリッジ インターフェースへの L2 ブリッジの有効化
- SNMP の有効化と SNMP マネージャ システムのトラップ送信先 IP アドレスの設定
- LAN トラフィックのセキュリティ サービスの設定
- “警告”またはそれ以下のレベルのログ警告の設定
- スイッチ上のミラーリングされたポートをブリッジ ペアの 1 インターフェースへ接続
- インターネット経由で動的シグネチャ データを取得するための WAN の接続と設定

プライマリ ブリッジ インターフェースの設定

プライマリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. X2 インターフェースの右の列にある**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**ゾーン**」ドロップダウン メニューから「**LAN**」を選択します。追加のオプションが表示されます。
   ⓘ | **補足:** 「**詳細設定**」タブまたは「**VLAN フィルタリング**」タブで設定を行う必要はありません。
4. 「**IP 割り当て**」で「**静的 IP モード**」を選択します。
5. インターフェースに静的 IP アドレス（`10.1.2.3` など）を設定します。ここで選択する IP アドレスが、スイッチから見える他のネットワークの IP アドレスと衝突しないように注意してください。
   ⓘ | **補足:** プライマリ ブリッジ インターフェースには、静的 IP を割り当てる必要があります。
6. **サブネット マスク**を設定します。
7. わかりやすい「**コメント**」を入力します。
8. インターフェースに対する「**管理**」オプションを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** の中から 1 つ以上の管理オプションを選択します。
9. 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。
10. HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「*HTTP/HTTPS リダイレクト*」

を参照してください。

11. 「OK」を選択します。

セカンダリ ブリッジ インターフェースの設定

ここでは、例として X3 をセカンダリ ブリッジ インターフェースとして使用します。

セカンダリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. X2 インターフェースの右の列にある**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**ゾーン**」ドロップダウン メニューから「**LAN**」を選択します。追加のオプションが表示されます。
   ⓘ | **補足:** 「**詳細設定**」タブまたは「**VLAN フィルタリング**」タブで設定を行う必要はありません。
4. 「**ネットワーク モード**」で、「**レイヤ 2 ブリッジ モード**」を選択します。
5. 「**ブリッジ先**」で、「**X2**」インターフェースを選択します。
6. IPv4 以外のトラフィックを監視する場合は、「**すべての非 IPv4 トラフィックを遮断する**」設定を有効にしないでください。
7. 「**このブリッジ ペアにトラフィックをルーティングしない**」チェックボックスをオンにして、ミラーリングされたスイッチ ポートからのトラフィックがネットワークに送り返されないようにします。
8. 「**このブリッジ ペアのトラフィックのみスニフする**」チェック ボックスをオンにして、ミラーリングされたスイッチ ポートから L2 ブリッジに到達したパケットのスニッファ、つまり監視を有効にします。
9. 「**このブリッジ ペアでステートフル インスペクションを無効にする**」を選択して、これらのインターフェースをステートフル高可用性検査から除外します。これらのインターフェースに対して精密パケット検査が有効になっている場合、DPI サービスは引き続き適用されます。
10. インターフェースに対する「**管理**」オプションを選択します。**HTTPS**、**Ping**、**SNMP**、**SSH** の中から 1 つ以上の管理オプションを選択します。
11. 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。
12. HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「*HTTP/HTTPS リダイレクト*」を参照してください。
13. 「**OK**」を選択します。

SNMP の構成

SNMP を有効にすると、侵入防御、ゲートウェイ アンチウイルス（GAV）などの SonicWall セキュリティ サービスによって生成される多くのイベントに際して自動的に SNMP トラップが発行されます。

現在、50 種類を超える IPS イベントと GAV イベントによって SNMP トラップが発行されます。『*SonicOS ログ管理ガイド*』には SonicOS でログを記録するイベントのリストがあり、各イベントに対応する SNMP トラップ番号も記載されています。このガイドは、SonicOS を実行している SonicWall プラットフォームを選択することによって、オンライン（https://www.sonicwall.com/ja-jp/support/technical-documentation/）で参照できます。

侵入防御を有効にして IPS スニッファ モードを使用する場合にトラップが発行可能かどうかを確認するには、『*SonicOS ログ管理ガイド*』の「ログ イベント メッセージのインデックス」セクションにある表で "**侵入**" を検索します。イベントに対応する SNMP トラップ番号があれば、表の「**SNMP トラップ タイプ**」列に記載されています。

ゲートウェイ アンチウイルスを有効にして IPS スニッファ モードを使用する場合にトラップが発行可能かどうかを確認するには、表で "**セキュリティ サービス**" を検索し、「**SNMP トラップ タイプ**」列の SNMP トラップ番号を確認します。

SNMP を有効にし、設定するには、以下の手順を行います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**SNMP を有効にする**」を選択します。
3. 「**適用**」を選択します。「**構成**」が使用可能になります。
4. 「**設定**」を選択します。「**SNMP ビュー構成**」ダイアログが表示されます。
5. 「**システム名**」フィールドに、セキュリティ装置から送信されるトラップを受け取る SNMP マネージャ システムの名前を入力します。
6. 「**システムの連絡先**」フィールドに SNMP 連絡先の担当者の名前または電子メール アドレスを入力します。
7. 「システムの場所」フィールドに、システムの場所を説明する文（「**3 階研究室**」など）を入力します。
8. 「**アセット番号**」フィールドに、システムのアセット番号を入力します。
9. 「**Get コミュニティ名**」フィールドに、SNMP 情報をファイアウォールから受け取る権限を持つコミュニティ名（「パブリック」など）を入力します。
10. 「**Trap コミュニティ名**」フィールドに、SNMP トラップをファイアウォールから SNMP マネージャに送信する際に使うコミュニティ名（「パブリック」など）を入力します。
11. 「**ホスト 1/2/3/4**」の各フィールドに、トラップを受け取る SNMP マネージャ システムの IP アドレスを入力します。
12. 「**OK**」を選択します。

IPS スニッファ モードの設定

IPS スニッファ モードを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. **X2** インターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**モード/IP 割り当て**」を「**レイヤ 2 ブリッジ モード**」に設定します。オプションが次のように変化します。
4. 「**ブリッジ先:**」インターフェースを「**X0**」に設定します。
5. 「**このブリッジ ペアのトラフィックのみスニフする**」を選択します。
6. 「**OK**」を選択すると、変更内容が保存されて有効になります。ダイアログが閉じられ、「**ネットワーク | システム > インターフェース**」ページが再び表示されます。
7. **X1 WAN** インターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
8. X1 WAN インターフェースにネットワークの内部 LAN セグメントの一意の IP アドレスを割り当てます。変に思われるかもしれませんが、実はこれが装置を管理するときに使うインターフェースです。また、このインターフェースからセキュリティ装置は SNMP トラップを送信し、セキュリティ サービス シグネチャの更新を取得します。
9. 「**OK**」を選択します。
10. また、トラフィックが正常に伝わるように、ファイアウォール ルールを変更して次の方向のトラフィックを許可してください。
    - LAN から WAN
    - WAN から LAN

11. 次のように接続します。
    - スパン/ミラー スイッチ ポートをセキュリティ装置の X2 ではなく X0 に接続（実際、X2 には何も接続されない）
    - X1 を内部ネットワークに接続

ⓘ | **重要:** ポートをスパニング/ミラーリングして X0 に接続するときは慎重にプログラミングしてください。

ⓘ | **補足:** 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、『*How to configure the SonicWall WAN / X1 Interface with PPPoE Connection (SonicWall WAN / X1 インターフェース を PPPoE 接続に設定する方法)*』をご覧ください。その他のビデオは、https://support.SonicWall.com/ja-jp/videos-product-select でご覧いただけます。

セキュリティ サービス(統合脅威管理)の設定

このセクションで有効にする設定に基づいて、IPS スニッファ モードで検知できる悪意のあるトラフィックの種類が決まります。一般には少なくとも 侵入防御 を有効にしますが、ゲートウェイ アンチウイルス、アンチスパイウェアなどの他のセキュリティ サービスを有効にしてもよいでしょう。

セキュリティ サービスを有効にするには、SonicWall セキュリティ装置のライセンスを取得し、シグネチャ情報を SonicWall データ センターからダウンロードする必要があります。侵入防御、ゲートウェイ アンチウイルス、アンチスパイウェアの有効化と設定の完全な手順については、『*SonicOS セキュリティ サービス管理ガイド*』を参照してください。

トピック:

- ログの設定
- ミラーリングされたスイッチ ポートの IPS スニッファ モード インターフェースへの接続
- データ センターに接続する WAN インターフェースの設定

ログの設定

「**デバイス | ログ > 設定**」ページでログを設定して、ファイアウォールで検知された攻撃についての情報を記録することができます。ログを有効にする方法については、『*SonicOS ログ管理ガイド*』を参照してください。

ミラーリングされたスイッチ ポートの IPS スニッファ モード インターフェースへの接続

標準の CAT-5 イーサネット ケーブルを使って、ミラーリングされたスイッチ ポートとブリッジ ペアのいずれかのインターフェースを接続します。ネットワーク トラフィックは、スイッチから装置に自動的に送信されます。装置ではトラフィックを検査できます。

ミラーリングされたポートの設定手順については、スイッチのドキュメントを参照してください。

データ センターに接続する WAN インターフェースの設定

セキュリティ装置の WAN ポート（通常はポート X1）をゲートウェイまたはゲートウェイにアクセスできる機器に接続します。装置は、SonicWall データ センターと自動的に通信します。WAN インターフェースを設定する詳細な手順については、「*WAN インターフェースの設定*」を参照してください。

ワイヤ モードとタップ モードの設定

トピック:

- ワイヤ モードでのインターフェースの設定
- WAN/LAN ゾーン ペアに対するワイヤ モードの設定
- ワイヤ モードでのリンク統合の設定

SonicOS はワイヤ モードとタップ モードをサポートしており、これにより全体的な中断を伴わずにネットワークへの挿入を段階的に増やす形で進めることができます。「ワイヤ モードとタップ モードの設定」で、ワイヤ モードとタップ モードについて説明します。

ワイヤ モードとタップ モードの設定

ワイヤ モード設定	説明
バイパス モード	バイパス モードにより、ネットワークへの装置ハードウェアの迅速で比較的中断のない導入が可能になります。ネットワークへ挿入するポイント（例: コア スイッチと境界装置の間、VM サーバ ファームの前、データ分類ドメイン間の移行ポイント）を選択すると、装置は物理データ パスに挿入され、必要となる整備期間が非常に短くなります。装置上のスイッチ ポートの 1 つ以上のペアが、すべてのパケットをセグメントを越えて完全なライン速度で転送するために使われます。すべてのパケットは、マルチコア検査および強制パスに搬送されるのではなく、装置の 240Gbps スイッチ ファブリック上に残ります。バイパス モードは検査やファイアウォール機能を提供しないので、このモードによって最小のダウンタイムと危険をもって装置をネットワークに物理的に導入して、ネットワークおよびセキュリティ インフラの新しく挿入された構成要素である水準の安心感を得ることができます。その後、再設定を行うための簡素なユーザ インターフェースを通してバイパス モードから検査または保護モードに即座に移行できます。
検査モード	検査モードは、低リスク、遅延の無いパケットパスなどの機能を変えることなくバイパスモードを拡張します。パケットは装置のスイッチ ファブリックを通過し続けますが、それらはまた、パッシブ検査、分類、フロー報告の目的のために、マルチコア RF-DPI エンジンにミラーされます。これは、実際の中間処理なしでのセキュリティ装置のアプリケーション情報および脅威検出機能を示します。
保護モード	保護モードは、検査モードを進化させたもので、装置のマルチコア プロセッサをパケット処理パスに積極的に介入させます。これは、アプリケーション情報と制御、侵入防御、ゲートウェイ アンチウイルス および クラウド ゲートウェイ アンチウイルス、アンチスパイウェア、そしてコンテンツ フィルタを含む、検査とポリシー エンジンの完全な機能セットを開放します。保護モードは、通常の NAT や L2 ブリッジ モードの配備と同じレベルの可視性と強制を、L3/L4 変換なしで、そして ARP やルーティング動作の変更なしで提供します。こうして保護モードは、既存のネットワーク設計への最低限の物理的変更だけで論理的変更を必要としない、少しずつ到達可能な NGFW 配備を提供します。 VLAN 変換のためにワイヤ モード ペアを作成するとき保護モードを使用してください。
タップ モード	タップ モードは検査モードと同じ可視性を提供しますが、装置上の単一スイッチ ポートを介してミラーされたパケット ストリームを吸収して、物理的な中間挿入の必要性を除去する点が異なります。タップ モードは、検査や収集用に外部機器にパケットを届けるためにネットワーク タップ、スマート タップ、ポート ミラー、また

ワイヤ モード設定	説明
	は、SPAN ポートを利用する環境で使用するように設計されています。ワイヤ モードの他のすべての形態と同様に、タップ モードは複数同時ポート インスタンスで動作可能で、複数タップからの不連続ストリームをサポートします。

ワイヤ モード:「機能の違い」は、インターフェース設定モード間の主な機能の違いを要約したものです。

ワイヤ モード: 機能の違い

インターフェース設定	バイパス モード	検査モード	保護モード	タップ モード	L2 ブリッジ、トランスペアレント、NAT、ルート モード
アクティブ/アクティブ クラスタリング	無	無	無	無	有
アプリケーション制御	無	無	有	無	有
アプリケーション可視化	無	有	有	有	有
ARP/ルーティング/NAT[a]	無	無	無	無	有
統合アンチスパム サービス[a]	無	無	無	無	有
コンテンツ フィルタ	無	無	有	無	有
DHCP サーバ[a]	無	無	無	無	有[b]
DPI 検出	無	有	有	有	有
DPI 防御	無	無	有	無	有
DPI-SSH[a]	無	無	有	無	有
高可用性	有	有	有	有	有
リンク状況伝播[c]	有	有	有	無	無
ステートフル パケット検査	無	有	有	有	有
TCP ハンドシェイク強制[d]	無	無	無	無	有
仮想グループ[a]	無	無	無	無	有
VLAN 変換[e]	無	無	有	無	無

ⓘ **補足:** ワイヤ モードで動作しているときは、ファイアウォール専用の管理インターフェースがローカル管理に使われます。リモート管理および動的なセキュリティ サービスとアプリケーション情報の更新を有効にするには、WAN インターフェース(ワイヤ モード インターフェースから独立した)をインターネット接続のために設定する必要があります。これは、SonicOS がほぼすべての組み合わせの混在モードのインターフェースをサポートするので、簡単にできます。

[a] これらの機能とサービスは、ワイヤ モードで設定されたインターフェースでは利用できませんが、システム全体レベルでは、他の互換性のある動作モードで設定されたどのインターフェースでも利用可能です。

[b] L2 ブリッジ モードでは利用不可です。

[c] **リンク状況伝播**は、ワイヤ モード ペアのインターフェースがパートナーの遷移によってトリガーされたリンク状況をミラー化する機能です。これは、冗長化パスのあるネットワークで正しい動作をするために不可欠です。リンク状況伝播は VLAN インターフェース越しのワイヤ モードではサポートされていません。

[d] ワイヤ モードでは、複数のワイヤ モードのパスまたは複数のセキュリティ装置が冗長または非対称パスと共に使用されている場合に、ネットワーク上のどこかで発生するフェイルオーバー イベントがサポートされることを許可するために、設計上無効になっています。

[e] VLAN 変換は VLAN インターフェース越しのワイヤ モードではサポートされていません。

ワイヤ モードでのインターフェースの設定

ワイヤ モードは、WAN、LAN、DMZ、および個別ゾーン（無線ゾーンを除く）に対して設定可能です。ワイヤ モードはレイヤ 2 ブリッジ モードを簡潔にしたもので、インターフェースのペアとして設定されます。ワイヤ モードでは、送信先ゾーンは「**ペア インターフェース ゾーン**」です。送信元の「**ゾーン**」とその「**ペア インターフェース ゾーン**」間のトラフィックの方向に基づいて、アクセス ルールがワイヤ モード ペアに適用されます。例えば、送信元の「**ゾーン**」が「**WAN**」で、「**ペア インターフェース ゾーン**」が「**LAN**」の場合、トラフィックの方向に応じて WAN から LAN へのルールと LAN から WAN へのルールが適用されます。

ワイヤ モードでは、インターフェースのリンク状況をペア インターフェースに伝播する**リンク状況伝達**を有効にすることができます。インターフェースが停止すると、そのインターフェースのリンク状況をミラーリングするために、対応するペア インターフェースが強制的に停止されます。ワイヤ モード ペアのインターフェースは、どちらも常に同じリンク状況になります。

ワイヤ モードでは、**ステートフル検査を無効**にできます。「**ステートフル検査を無効にする**」を選択すると、ステートフル パケット検査がオフになります。「**ステートフル検査を無効にする**」が選択されていない場合は、3 ウェイ TCP ハンドシェイクを強制することなく、新しい接続を確立できます。非対称ルートを配備する場合は、「**ステートフル検査を無効にする**」を選択する必要があります。

インターフェースをワイヤ モード用に設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. ワイヤ モード用に設定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**ゾーン**」で、WLAN 以外の任意のゾーン種別を選択します。
4. 「**モード / IP 割り当て**」で、次のように選択してインターフェースを設定します。
   - タップ モードの場合、「**タップ モード (1 ポート タップ)**」を選択
   - ワイヤ モードの場合、「**ワイヤ モード (2 ポート ワイヤ)**」を選択
5. 「**ワイヤ モード種別**」で、適切なモードを選択します。
   - **バイパス (内部スイッチ/リレーによる)**
   - **検査 (ミラー トラフィックのパッシブ DPI)**
   - **保護 (直列トラフィックのアクティブ DPI)**
6. 「**ペア インターフェース**」で、上流のセキュリティ装置に接続するインターフェースを選択します。このペア インターフェースは同じ種別 (2 つの 1 GB インターフェースまたは 2 つの 10 GB インターフェース) である必要があります。

ⓘ | **補足:** 未定義のインターフェースのみが、「**ペア インターフェース**」で利用可能です。インターフェースを未定義にするには、そのインターフェースの「**設定**」を選択し、「**ゾーン**」で「**未定義**」を選択します。

7. 「**OK**」を選択します。

WAN/LAN ゾーン ペアに対するワイヤ モードの設定

以下の設定は、ワイヤ モードの設定例です。この例は、LAN ゾーンとペアリングされた WAN ゾーン向けです。ワイヤ モードは、DMZ ゾーンおよび個別ゾーンに対しても設定できます。

WAN/LAN ゾーン ペアに対してワイヤ モードを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 次のいずれかを選択します。
   - **インターフェースの追加**。
   - 設定するインターフェースの**設定**アイコン

   「**インターフェースの追加/編集**」ダイアログが表示されます。
3. 「**ネットワーク モード**」で、「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。
4. 「**ゾーン**」で、「**WAN**」を選択します。
5. 「**ペア インターフェース ゾーン**」で、「**LAN**」を選択します。
6. 「**ステートフル検査を無効にする**」を選択します。
7. 「**リンク状況伝播を有効にする**」を選択します。
8. 「**OK**」を選択します。「インターフェース設定」テーブルが更新されます。

ワイヤ モードでのリンク統合の設定

ⓘ | **補足:** VLAN インターフェース越しのワイヤ モードは、リンク統合をサポートしていません。

リンク統合 (LAG) は、複数のリンクを単一のインターフェースにバンドルして帯域幅を増やすために使用されます。LAG インターフェース上でトラフィックを検査するため、SonicWall セキュリティ装置をインラインで接続し、1 つのリンクに送信されるパケットを送信先に透過的にブリッジすることができます。リンク状況伝播などの既存のワイヤ モード機能がサポートされています。LAG ごとに最大 8 つのメンバーをサポートします。

ワイヤ モードでのリンク統合は、「**ネットワーク | システム > インターフェース**」で設定します。「**リンク統合**」が「**インターフェースの編集 > 詳細**」ダイアログで選択されている場合は、未定義のインターフェースもリストに表示されます。ワイヤ モード接続のそれぞれの側に対してメンバー インターフェースを選択できます。それぞれの側のメンバー数は同じでなければなりません。メンバー インターフェースのタイプと帯域幅サイズも一致させることをお勧めします。

ワイヤ モードでの LAG を設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 設定するインターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**ゾーン**」で、適切なゾーンを選択します。オプションが次のように変化します。
4. 「**モード / IP 割り当て**」で、「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。再びオプションが変化します。
5. 「**ワイヤ モード種別**」で、「**保護 (直列トラフィックのアクティブ DPI)**」を選択します。
6. 「**ペア インターフェース**」から、ペアにするインターフェースを選択します。

7. 「**ペア インターフェース ゾーン**」から、ペアにするインターフェースのゾーンを選択します。
8. 「**ステートフル検査を無効にする**」オプションを選択します。このオプションは、既定では選択されています。
9. 必要に応じて、「**リンク状況伝播を有効にする**」を選択します。このオプションは、既定では選択されていません。
10. 「**詳細**」を選択します。

「詳細設定」での設定を続行するには、以下の手順に従います。

1. 「**冗長/統合ポート**」で、「**リンク統合**」を選択します。オプションが次のように変化します。
2. 「**統合ポート**」で、統合するポートを選択します。
3. 「**ペア インターフェース統合ポート**」から、統合するペア ポートを選択します。
4. 「**OK**」を選択します。設定が「**ネットワーク | システム > インターフェース**」の「**インターフェース設定**」テーブルに表示されます。

レイヤ 2 ブリッジ モード

トピック:

- SonicOS レイヤ 2 ブリッジ モードの主要な機能
- L2 ブリッジ モードとトランスペアレント モードの設定に関連した重要な概念
- L2 ブリッジ モードとトランスペアレント モードの比較
- L2 ブリッジ パスの決定
- L2 ブリッジ インターフェース ゾーンの選択
- サンプル トポロジ
- ネットワーク インターフェースの設定と L2B モードの有効化
- レイヤ 2 ブリッジ モードの設定
- 非対称ルーティング

SonicOS には、セキュリティ装置をあらゆるイーサネット ネットワークに透過的に統合するための手法として、L2 (レイヤ 2) ブリッジ モードが備わっています。L2 ブリッジ モードは、セキュリティ装置が、2 つのインターフェース間で共通のサブネットを共有し、すべての IP トラフィックに対してステートフルな精密パケット検査を実行できるという点で、見かけ上は SonicOS のトランスペアレント モードに似ていますが、機能的にはより多目的な用途に対応しています。

L2 ブリッジ モードでは、セキュリティで保護された学習ブリッジ手法が採用されているため、他の多くの透過的な装置統合方式では処理できない種類のトラフィックを通過させ、検査することができます。L2 ブリッジ モードを使うと、既存のイーサネット ネットワークに影響を与えずに SonicWall セキュリティ装置を追加して、インラインの精密パケット検査機能をすべての IPv4 TCP と UDP のトラフィックに提供することができます。このシナリオでは、装置がセキュリティを適用するためではなく、両方向のスキャン、ウィルスとスパムの遮断、および侵入の阻止に使用します。

他の透過的なソリューションとは異なり、L2 ブリッジ モードは、IEEE 802.1Q VLAN、Spanning Tree Protocol、マルチキャスト、ブロードキャスト、IPv6 を含む、すべての種類のトラフィックを通過させるため、いずれのネットワーク通信も中断されることはありません。

L2 ブリッジ モードの多目的性を示すもう 1 つの例が、このモードを使用して IPS スニッファ モードを設定できることです。IPS スニッファ モードは、SonicWall セキュリティ装置でサポートされ、ブリッジ ペアの 1 インターフェースを使用してスイッチ上のミラーリングされたポートからのネットワーク トラフィックを監視します。IPSスニッファ モードでは侵入検知が可能ですが、装置がトラフィック フローにインラインで接続されていないため、悪意のあるトラフィックを遮断することはできません。詳細については、「IPS スニッファ モード」を参照してください。

L2 ブリッジ モードは、既存の装置が存在し、既存の装置を変更する計画が当面はなく、一方で SonicWall 精密パケット検査とセキュリティ サービスのセキュリティ機能 (侵入防御、ゲートウェイ アンチウイルス、アンチスパイウェアなど) を追加する必要のあるネットワークにとって理想的なソリューションです。SonicWall セキュリティ サービスを購読していない場合は、MySonicWall で無料トライアルに申し込むことができます。

L2 ブリッジ モードは高可用性を備えた配備でも使用できます。このシナリオについては、「*高可用性を備えたレイヤ 2 ブリッジ モード*」で説明します。

ⓘ | **補足:** リンク統合は、レイヤ 2 ブリッジ モードではサポートされません。

SonicOS レイヤ 2 ブリッジ モードの主要な機能

SonicOS レイヤ 2 ブリッジ モード: 「主要な機能と利点」は、レイヤ 2 ブリッジ モードの主要な機能とその利点をまとめたものです。

SONICOS レイヤ 2 ブリッジ モード: 主要な機能と利点

機能	利点
精密パケット検査を備えた L2 ブリッジング	アドレスの再割り当てや再構成を行うことなく、SonicWall セキュリティ装置をあらゆるネットワークに追加でき、かつ、既存のネットワーク デザインを変更することなく、精密パケット検査のセキュリティ サービスを追加できるトランスペアレントな処理手法です。L2 ブリッジ モードは、セキュリティと同程度に接続性を重視して設計され、あらゆる種類のイーサネット フレームを通過させることができるため、シームレスな統合が可能となります。
セキュリティで保護された学習ブリッジ手法	許可されているすべてのトラフィックが L2 ブリッジを介してネイティブに通過できなければ、真の L2 動作とは言えません。L2 ブリッジ モード以外のトランスペアレント処理手法は、透過性を実現するために ARP やルート操作に依存しており、そのことが原因で問題が生じることも少なくありません。これに対し、L2 ブリッジ モードでは、ネットワークのトポロジを動的に学習することによって最適なトラフィック パスが決定されます。
あらゆるイーサネット フレーム タイプのサポート	すべてのイーサネット トラフィックが L2 ブリッジを通過できます。つまり、どのようなネットワーク通信も中断されることはありません。その他多くのトランスペアレント処理手法が IPv4 トラフィックしかサポートしていないのに対し、L2 ブリッジ モードは、すべての IPv4 トラフィックを検査したうえで、その他すべてのトラフィック (LLC、全 Ethertype、独自フレーム形式など) を通過させるか、必要であれば遮断します。
混在モード処理	L2 ブリッジ モードは、L2 ブリッジに加え、従来の装置のサービス (ルーティング、NAT、VPN、無線動作など) を同時に提供します。したがって、ネットワークの特定のセグメントでは L2 ブリッジとして使用しながら、それ以外のセグメントにはセキュリティ サービス一式をすべて提供するといったことも可能です。SonicWall セキュリティ装置をピュア L2 ブリッジとして導入しておき、将来、必要に応じて完全なセキュリティ サービス動作に移行させることもできます。
無線 レイヤ 2 ブリッジ	LAN、WLAN、DMZ、または個別ゾーンなど、複数のゾーン タイプにわたって単一の IP サブネットを使用します。この機能により、無線クライアントと有線クライアントは、DHCP アドレスなどの同じネットワーク リソースをシームレスに共有できます。レイヤ 2 プロトコルはペア インターフェースの間で動作可能で、ブロードキャスト パケットや非 IP パケットなど、複数のトラフィック種別がブリッジを通過できるようにします。

L2 ブリッジ モードとトランスペアレント モードの設定に関連した重要な概念

L2 ブリッジ モードの運用と設定について言及する際、次のような用語が使用されます。

L2 ブリッジ モード — SonicWall セキュリティ装置の設定手法の 1 つです。ファイアウォールをインラインで既存のネットワークに追加でき、トランスペアレント モードを超える完全な透過性を実現します。レイヤ 2 ブリッジ モードは、ブリッジ ペアのセカンダリ ブリッジ インターフェースに対して選択されたネットワーク モード設定と言うこともできます。

トランスペアレント モード — SonicWall セキュリティ装置の設定方法の 1 つです。自動的に適用される ARP とルーティング ロジックを使用し、単一の IP サブネットを複数のインターフェースにスパニングすることにより、IP を設定し直すことなく、セキュリティ装置を既存のネットワークに追加できるようにします。

ネットワーク モード — 保護インターフェース (LAN) またはパブリック インターフェース (DMZ) を設定するとき、インターフェースのネットワーク モードとして、次のいずれかを選択できます。

静的 — インターフェースの IP アドレスを手動で入力します。

トランスペアレント モード — インターフェースの IP アドレスが、WAN プライマリ IP サブネット範囲内のアドレス オブジェクト (ホスト、範囲、またはグループ) を使って割り当てられ、WAN インターフェースから、割り当てられているインターフェースへとサブネットを効果的にスパニングすることができます。

レイヤ 2 ブリッジ モード — このモードで設定されたインターフェースは、同じブリッジ ペアのプライマリ ブリッジ インターフェースに対するセカンダリ ブリッジ インターフェースになります。このブリッジ ペアは、完全な L2 透過性を備えた 2 ポートの学習ブリッジのように振る舞い、それを通過するすべての IP トラフィックは完全なステートフル フェイルオーバーと精密パケット検査の対象となります。

ブリッジ ペア — プライマリ ブリッジ インターフェースとセカンダリ ブリッジ インターフェースの組み合わせから成る論理的なインターフェースです。ここで言うプライマリとセカンダリは、本質的な動作上の優位性や主従関係を表すものではありません。どちらのインターフェースも絶えずそれぞれのゾーン タイプに従って扱われ、設定されているアクセス ルールに従って IP トラフィックを通過させます。ブリッジ ペアを通過する非 IPv4 トラフィックは、セカンダリ ブリッジ インターフェースの「すべての非 IPv4 トラフィックをブロックする」の設定によって制御されます。サポートされるブリッジ ペアの数は、利用可能なインターフェースのペアに依存します。つまり、ブリッジ ペアの最大数は、プラットフォーム上の物理インターフェース数を 2 で割った値になります。ブリッジ ペアに属しているからといって、インターフェースの従来の動作が妨げられることはありません。例えば、X1 が、X3 をセカンダリ ブリッジ インターフェースとするブリッジ ペアのプライマリ ブリッジ インターフェースとして設定されている場合、X1 は、同時にプライマリ WAN としての従来の役割を果たし、自動的に追加される X1 の既定 NAT ポリシーを介して、インターネット宛てのトラフィックの NAT 変換を実行できます。

プライマリ ブリッジ インターフェース — セカンダリ ブリッジ インターフェースと対をなすインターフェースの呼称です。プライマリ ブリッジ インターフェースは、非保護ゾーン (WAN)、保護ゾーン (LAN)、パブリック ゾーン (DMZ) のいずれかに所属することができます。

セカンダリ ブリッジ インターフェース — ネットワーク モードがレイヤ 2 ブリッジ モードに設定されたインターフェースの呼称です。セカンダリ ブリッジ インターフェースは、保護ゾーン (LAN) またはパブリック ゾーン (DMZ) に所属することができます。

ブリッジ管理アドレス — プライマリ ブリッジ インターフェースのアドレスは、ブリッジ ペアの両方のインターフェースによって共有されます。プライマリ ブリッジ インターフェースがプライマリ WAN インターフェースとしても機能する場合、装置の発信通信 (NTP など) やライセンス マネージャの更新には、このアドレスが使用されます。また、混在モードの配備において、ブリッジ ペアのいずれかのセグメントに接続されたホストが、そのゲートウェイとしてブリッジ管理アドレスを使用する場合もあります。

ブリッジ パートナー — ブリッジ ペアのもう一方のメンバーを指す用語です。

非 IPv4 トラフィック – SonicOS は以下の IP プロトコル種別をサポートします。ICMP (1)、IGMP (2)、TCP (6)、UDP (17)、GRE (47)、ESP (50)、AH (51)、EIGRP (88)、OSPF (89)、PIM-SM (103)、L2TP (115)。Combat Radio Transport Protocol (126) などの特殊な IP 種別や IPX、(現時点では) IPv6 などの非 IPv4 トラフィック種別については、装置でネイティブに処理することはできません。非 IPv4 トラフィックは、L2 ブリッジ モードの設定により通過させるか破棄することができます。

キャプティブ ブリッジ モード — L2 ブリッジ動作のこのオプション モードでは、L2 ブリッジに到着したトラフィックを非ブリッジ ペア インターフェースに転送することができません。既定では、L2 ブリッジのロジックにより、L2 ブリッジに到着したトラフィックは ARP およびルーティング テーブルによって決定される最適なパスに従って送信先に転送されます。場合によっては、こうした最適なパスで非ブリッジ ペア インタフェースへのルーティングや NAT 変換が必要になることがあります。キャプティブ ブリッジ モードを有効にすると、L2 ブリッジに到着するトラフィックは論理的に最適なパスを取ることなく L2 ブリッジを出て行きます。一般に、このモードの動作が必要になるのは、冗長なパスが存在する複雑なネットワークでパスの厳守が求められる場合に限られます。

ピュア L2 ブリッジ トポロジ — ネットワークにインライン セキュリティを提供することを目的とし、セキュリティ装置を厳密な L2 ブリッジ モードで使用することをいいます。つまり、ブリッジ ペアの一方の側に着信したトラフィックは常にもう一方の側に宛てて送出されます。異なるインターフェースを介してルーティングまたは NAT 変換されることはありません。既に境界装置が存在する場合や、既存のネットワークの特定のパス (部門間または 2 つのスイッチ間のトランク リンクなど) に沿ったインライン セキュリティが求められる場合に用いられる代表的なトポロジです。ピュアL2 ブリッジ トポロジは機能的な制約を意味するものではなく、むしろ混成環境における一般的な配備を表すトポロジ上の概念と言えます。

混在モード トポロジ — 装置を介した受信/送信のポイントがブリッジ ペア以外にも存在する配備をいいます。つまり、ブリッジ ペアの一方の側に着信したトラフィックは、異なるインターフェースを介してルーティングまたは NAT 変換されることもあります。例えば、次のような環境が既に整っているとき、同時に装置を使用することで、1 つまたは複数のブリッジ ペアにセキュリティを提供できます。

- ブリッジ ペアまたは他のインターフェース上のホストに対する境界セキュリティ (WAN 接続など)。
- 保護 (LAN) インターフェースや公開 (DMZ) インターフェースなど、追加のセグメントに対するファイアウォールやセキュリティ サービス。この場合、これらのセグメント上のホストと、ブリッジ ペア上のホストとの間で通信を行うことになります。
- SonicPoint による無線サービス。この場合、無線クライアントと、ブリッジ ペア上のホストとの間で通信が行われます。

L2 ブリッジ モードとトランスペアレント モードの比較

トランスペアレント モードでは、SonicOS が実行されている装置を、アドレスの再割り当てなしに既存のネットワークに導入できますが、この場合、特に ARP、VLAN サポート、複数サブネット、非 IPv4 トラフィック種別に関して、ある程度の中断を伴います。例えば、統合に伴う中断を最小限に抑えることを優先し、トランスペアレント モードの SonicWall セキュリティ装置をネットワークに追加したとします。この構成の特徴を次に示します。

- 予定外のダウンタイムがまったく発生しないか、発生したとしても無視できるほど小さい。
- ネットワークのどの部分にもアドレスの再割り当てが不要。
- (ルータが ISP によって所有されている場合によく見られるような) ゲートウェイ ルータの再設定や変更が不要。

トピック:

- L2 ブリッジ モードとトランスペアレント モードの比較
- L2 ブリッジ モードにはないトランスペアレント モードのメリット
- トランスペアレント モードでの ARP
- トランスペアレント モードの VLAN サポート
- トランスペアレント モードでの複数サブネット
- トランスペアレント モードの非 IPv4 トラフィック
- L2 ブリッジ モードでの ARP
- L2 ブリッジ モードでの VLAN サポート
- L2 ブリッジの IP パケット パス
- L2 ブリッジ モードでの複数サブネット
- L2 ブリッジ モードでの非 IPv4 トラフィック

L2 ブリッジ モードとトランスペアレント モードの比較

L2 ブリッジ モードとトランスペアレント モードの比較

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
動作のレイヤ	レイヤ 2 (MAC)	レイヤ 3 (IP)
ARP 動作	ARP (Address Resolution Protocol) の情報は変更されません。MAC アドレスはそのままの形で L2 ブリッジを通過します。SonicWall セキュリティ装置の MAC アドレスを宛先とするパケットは処理され、それ以外のパケットは通過します。送信元と送信先が学習されてキャッシュされます。	ARP は、トランスペアレント モードで動作するインターフェースによってプロキシされます。
パスの決定	ブリッジ ペアのいずれかの側のホストが、動的に学習されます。インターフェースの関連付けを宣言する必要はありません。	プライマリ WANインターフェースは、常にトランスペアレント モード トラフィックおよびサブネット空間決定のマスター受信/送信ポイントになります。このサブネット空間を透過的に共有するホストは、アドレス オブジェクトの割り当てを使用して明示的に宣言されている必要があります。
最大インターフェース数	2 つ (プライマリ ブリッジ インターフェースおよびセカンダリ ブリッジ インターフェース)。	複数のインターフェース。マスター インターフェースは常にプライマリ WANになります。利用可能なインターフェースさえあれば、従属トランスペアレント インターフェースの数に制限はありません。
最大ペア数	最大数ブリッジ ペア数は、利用可能な物理インターフェース数に依存します。これは、"複数の 1 対 1 ペアリング" と考えることができます。	トランスペアレント モードでは、複数のインターフェースが同時にプライマリ WANに対するトランスペアレント パートナーとして動作することはできますが、これは単にプライマリ WANのサブネットを他のインターフェースにスパニングしているに過ぎません。これは、"単一の 1 対 1 ペアリング" または "単一の 1 対多ペアリング" と考えることができます。
ゾーンの制限	プライマリ ブリッジ インターフェースは、	トランスペアレント モード ペアのインター

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
	非保護、保護、パブリックのいずれかになります。セカンダリ ブリッジ インターフェースは、保護またはパブリックのいずれかになります。	フェースは、1 つの非保護インターフェース（ペアのサブネットのマスターとしてのプライマリ WAN）と、1 つ以上の保護/パブリック インターフェース（LAN または DMZ など）で構成されている必要があります。
サポートされるサブネット数	任意の数のサブネットがサポートされます。サブネットへのトラフィックまたはサブネットからのトラフィックは、アクセス ルールを作成することによって制御できます。	既定の設定では、トランスペアレント モードでサポートされるサブネット数は 1 つだけです（つまり、プライマリ WANに割り当てられ、プライマリ WANからスパニングされるサブネット）。ARP エントリおよびルートを使用して、サブネットを手動で追加することはできます。
非 IPv4 トラフィック	既定では、セカンダリ ブリッジ インターフェースの設定ページで無効にされていない限り、すべての非 IPv4 トラフィックが、ブリッジ ペア インターフェースからそのブリッジ パートナー インターフェースへとブリッジされます。これには、IPv6 トラフィック、STP (Spanning Tree Protocol)、および識別不能の IP タイプも含まれます。	トランスペアレント モードでは非 IPv4 トラフィックは処理されません。破棄されてログに記録されます。
VLAN トラフィック	VLAN トラフィックは L2 ブリッジを介して渡され、ステートフル精密パケット検査エンジンによって完全に検査されます。	VLAN サブインターフェースを作成し、トランスペアレント モード アドレス オブジェクトを割り当てることはできますが、VLAN はそのまま通過するのではなく、セキュリティ装置で終端されます。
VLAN サブインターフェース	ブリッジ ペア インターフェース上で VLAN サブインターフェースを作成することはできます。ただし、VLAN フレーム内の送信先 IP アドレスが、装置上の VLAN サブインターフェースの IP アドレスと一致しない限り、VLAN サブインターフェースは、ブリッジを介してブリッジ パートナーへと渡されます。両者のアドレスが一致した場合は（例えば、管理トラフィックとして）処理されます。	トランスペアレント モードで動作する物理インターフェースに VLAN サブインターフェースを割り当てることはできますが、動作モードはその親に依存しません。これらの VLAN サブインターフェースに、トランスペアレント モード アドレス オブジェクトを割り当てることもできますが、VLAN サブインターフェースはそのまま通過するのではなく終端されます。
動的アドレッシング	プライマリ ブリッジ インターフェースを WANゾーンに割り当てることはできますが、プライマリ ブリッジ インターフェースに対しては静的アドレッシングしか行えません。	トランスペアレント モードでは、プライマリ WANがマスター インターフェースとして使用されますが、トランスペアレント モードでは静的アドレッシングしか許可されません。
VPN サポート	ルート設定を 1 つ追加することで VPN 動作がサポートされます。詳細については、「*レイヤ 2 ブリッジ モードでの VPN 統合*」を参照してください。	VPN 動作がサポートされます。特別な設定要件はありません。
DHCP サポート	DHCP はブリッジ ペアを通過できます。	トランスペアレント モードで動作するインター

項目	レイヤ 2 ブリッジ モード	トランスペアレント モード
		フェースは、DHCP サービスを提供するか、IP ヘルパーを使って DHCP を通過させることができます。
ルーティングと NAT	L2 ブリッジ ペアと他のパス間のトラフィックはインテリジェントにルーティングされます。既定では、ブリッジ ペア インターフェースからブリッジ パートナーへのトラフィックは NAT 変換されませんが、他のパスへのトラフィックを必要に応じて NAT 変換することもできます。必要に応じて独自のルートおよび NAT ポリシーを追加できます。	他のパスとの間のトラフィックはインテリジェントにルーティングされます。既定では、WAN とトランスペアレント モード インターフェース間のトラフィックは NAT 変換されませんが、他のパスへのトラフィックを必要に応じて NAT 変換することもできます。必要に応じて独自のルートおよび NAT ポリシーを追加できます。
ステートフル パケット検査	ファイアウォールの VLAN トラフィックなど、L2 ブリッジを通過するすべてのサブネットのすべての IPv4 トラフィックには、完全なステートフル パケット検査が適用されます。	トランスペアレント モード アドレス オブジェクトの割り当てによって定義されたサブネットへのトラフィックおよびサブネットからのトラフィックには、完全なステートフル パケット検査が適用されます。
セキュリティ サービス	すべてのセキュリティ サービス（GAV、IPS、アンチスパイウェア、CFS）が完全にサポートされます。これには、標準的な IP トラフィックと 802.1Q カプセル化 VLAN トラフィックがすべて含まれます。	トランスペアレント モード アドレス オブジェクトの割り当てによって定義されたサブネットとの間で、すべてのセキュリティ サービス（GAV、IPS、アンチスパイウェア、CFS）が完全にサポートされます。
ブロードキャスト トラフィック	ブロードキャスト トラフィックは、受信したブリッジ ペア インターフェースからブリッジ パートナー インターフェースへと渡されます。	ブロードキャスト トラフィックは破棄されてログに記録されます。ただし、NetBIOS については、IP ヘルパーによって処理される場合があります。
マルチキャスト トラフィック	「**ネットワーク	システム > マルチキャスト**」でマルチキャストが有効にされている場合、マルチキャスト トラフィックは検査され、L2 ブリッジ ペアを介して渡されます。IGMP メッセージングには依存せず、個々のインターフェースでマルチキャスト サポートを有効にする必要はありません。	「**ネットワーク	システム > マルチキャスト**」でマルチキャストが有効にされており、かつ、関連するインターフェースでマルチキャスト サポートが有効になっている場合、マルチキャスト トラフィック（IGMP に依存）は検査され、トランスペアレント モードで渡されます。

L2 ブリッジ モードにはないトランスペアレント モードのメリット

L2 ブリッジ ペアでは最大 2 つのインターフェースしか許容されません。3 つ以上のインターフェースを同じサブネット上で運用する必要がある場合は、トランスペアレント モードを検討することをお勧めします。

トランスペアレント モードでの ARP

トランスペアレント モードでは、ARP（Address Resolution Protocol: ネットワーク インターフェース カードの一意のハードウェア アドレスと IP アドレスとを関連付けるメカニズム）がプロキシされます。左側のワークステーションまたはサーバが、過去にルータ（`192.168.0.1`）の MAC アドレスを `00:99:10:10:10:10` に解決したことがある場合、これらのホストが装置を介して通信を行うためには、このキャッシュされた ARP 登録がクリアされている必要

があります。これは、装置が、トランスペアレント モード動作のインターフェースに接続されているホストに代わって、ゲートウェイの IP（192.168.0.1）をプロキシ（つまり、代理で応答する）するためです。したがって、左側のワークステーションが 192.168.0.1 の解決を試みるために ARP 要求を送信すると、装置が自分の X0 の MAC アドレス（00:06:B1:10:10:10）を返すことによって応答します。

同様に、装置がその X1（プライマリ WAN）インターフェースで ARP 要求を受信した場合、トランスペアレント モードのインターフェースに割り当てられたトランスペアレント範囲（192.168.0.100 ～ 192.168.0.250）に指定されている IP アドレスを対象に ARP のプロキシを行います。ルータが過去にサーバ（192.168.0.100）の MAC アドレスを 00:AA:BB:CC:DD:EE に解決したことがある場合、装置を介してホストと通信するためには、このキャッシュされた ARP 登録がクリアされている必要があります。通常、そのためには、管理インターフェースを使用するか、再起動することによって、ルータの ARP キャッシュを消去する必要があります。ルータの ARP キャッシュがクリアされると、このルータは、192.168.0.100 に対する新しい ARP 要求を送信できます。装置は、それに対する応答として、X1 の MAC アドレスである 00:06:B1:10:10:11 を返します。

トランスペアレント モードの VLAN サポート

上図のネットワークは単純なものですが、VLAN を使ってトラフィックをセグメント化する大規模なネットワークでは決して珍しくありません。スイッチとルータ間のリンクが VLAN トランクであるようなネットワークの場合、リンクのいずれかの側のサブインターフェースへの VLAN を、トランスペアレント モードの SonicWall セキュリティ装置で終端させることはできますが、一意のアドレス割り当てが必要となります。つまり、非トランスペアレント モードの動作となるため、少なくとも一方の側のアドレスを再割り当てする必要があります。これは、トランスペアレント モードのアドレス空間の送信元として使用できるのはプライマリ WAN インターフェースだけであるためです。

トランスペアレント モードでの複数サブネット

大規模なネットワークでは、単一の有線上、複数の有線上、別個の VLAN 上、またはそれらを組み合わせた回線上で、複数のサブネットが使用されることも少なくありません。トランスペアレント モードは、静的 ARP エントリとルート エントリを使って複数のサブネットをサポートできます。

トランスペアレント モードの非 IPv4 トラフィック

トランスペアレント モードでは、非 IPv4 トラフィックがすべて破棄（および通常はログに記録）されるため、他の種類のトラフィック（IPX など、処理されない IP タイプ）が通過することはできません。

L2 ブリッジ モードでの ARP

L2 ブリッジ モードには、どのホストが、L2 ブリッジ（ブリッジ ペア）のどのインターフェース上に存在するかを動的に調査する学習ブリッジ設計が採用されています。ARP はネイティブに通過します。つまり、L2 ブリッジを介して通信を行うホストからは、そのピアの実際のホスト MAC アドレスが見えます。例えば、ルータ（192.168.0.1）と通信しているワークステーションは、ルータを 00:99:10:10:10:10 として認識し、ルータはワークステーション（192.168.0.100）を 00:AA:BB:CC:DD:EE として認識します。

この動作により、L2 ブリッジ モードで動作する SonicWall セキュリティ装置は、物理的な挿入に伴う一時的な中断を除けば、ほとんどのネットワーク通信を中断させることなく、既存のネットワークに導入できます。

L2 ブリッジ モードの装置を挿入した場合は、ストリームベースの TCP プロトコル通信（クライアントとサーバ間の FTP セッションなど）を再度確立する必要があります。これは、ステートフル パケット検査によりもたらされるセキュリティを維持することを目的としています。ステートフル パケット検査エンジンは、自分より前に存在していた TCP 接続に関する情報を持ちません。そのため、これらの確立済みのパケットはログ イベント（存在しない接続または終了済みの接続で TCP パケットが受信されたために、その TCP パケットは破棄されたなど）を伴って破棄されます。

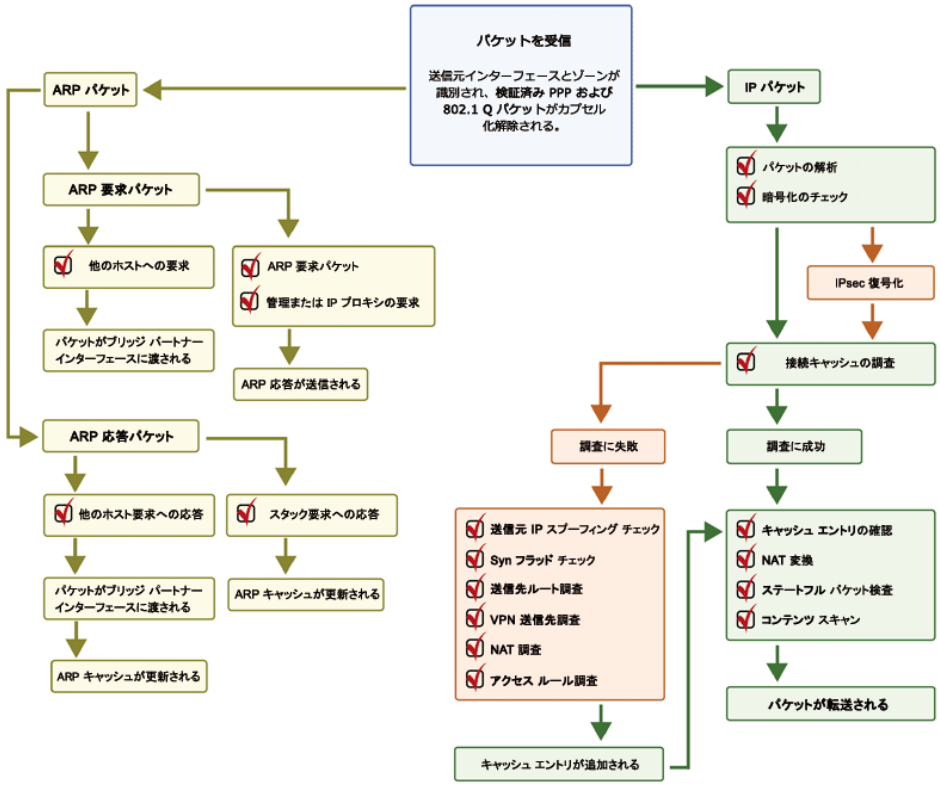
L2 ブリッジ モードでの VLAN サポート

SonicWall セキュリティ装置の L2 ブリッジ モードでは、L2 ブリッジを通過する 802.1Q VLAN トラフィックをきめ細かく制御できます。VLAN の既定の処理では、カプセル化されたトラフィックに、あらゆるファイアウォール ルール、および、ステートフル精密パケット検査を適用しながら、L2 ブリッジを通過するすべての 802.1Q VLAN タグが許可および維持されます。さらに、L2 ブリッジでは、許可/禁止された VLAN ID のホワイト/ブラック リストを指定することも可能です。

例えば、任意の数の VLAN を持つ VLAN トランクに対し、L2 ブリッジ モードで動作する装置をインラインで挿入し、いずれの VLAN ID またはサブネットにも明示的な設定を施すことなく、その VLAN を通過するすべての IPv4 トラフィックに完全なセキュリティ サービスを提供できます。VLAN トラフィックの処理手法により、必要であれば、L2 ブリッジ モード経由で通過するすべての VLAN トラフィックにアクセス ルールを適用することもできます。

L2 ブリッジの IP パケット パス

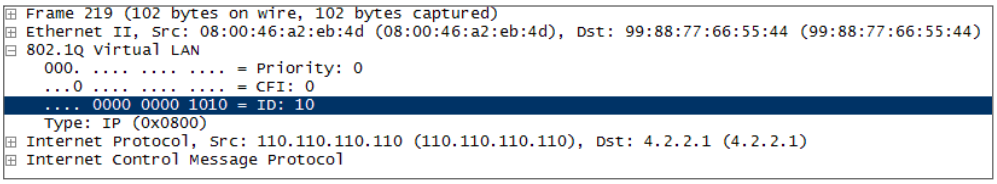
L2 ブリッジの IP パケット フロー



次のイベント シーケンスは、「L2 ブリッジの IP パケット フロー」:

1. 802.1Q カプセル化フレームが L2 ブリッジ インターフェースに到着します (このステップ 1、ステップ 2、およびステップ 12 は、802.1Q VLAN トラフィックにのみ当てはまります)。
2. 802.1Q VLAN ID が VLAN ID のホワイト/ブラック リストと照らしてチェックされます。VLAN ID:
    - 禁止されていた場合、パケットは破棄されてログに記録されます。
    - 許可されていた場合、パケットのカプセル化が解除され、VLAN ID が格納されて、内部パケット (IP ヘッダーを含む) がフル パケット ハンドラを介して渡されます。

3. L2 ブリッジでは任意の数のサブネットがサポートされるため、パケットの送信元 IP に対する送信元 IP スプーフィング チェックは実行されません。アクセス ルールを使って特定のサブネットだけをサポートするように L2 ブリッジを設定することもできます。
4. SYNフラッド チェックが実行されます。
5. 適切なアクセス ルールを適用するため、送信先ゾーンに対して送信先ルート調査が実行されます。送信元ゾーンと同じゾーン（LAN から LAN など）、非保護ゾーン（WAN）、暗号化（VPN）、無線（WLAN）、マルチキャスト、任意のタイプの個別ゾーンを含め、すべてのゾーンが有効な送信先になります。
6. NAT 調査が実行され、必要に応じて適用されます。
    - 一般に、L2 ブリッジに到達したパケットの送信先はブリッジ パートナー インターフェース（つまり、ブリッジのもう一方の側）です。この場合、変換は一切実行されません。
    - 混在モードのトポロジで多く見られるように、L2 ブリッジ管理アドレスがゲートウェイである場合、NAT が必要に応じて適用されます（詳細については、「*L2 ブリッジ パスの決定*」を参照してください）。
7. パケットにアクセス ルールが適用されます。例えば、SonicWall セキュリティ装置の場合、次のパケット デコードは、VLAN ID 10、送信元 IP アドレス `110.110.110.110`、送信先 IP アドレス `4.2.2.1` の ICMP パケットを示しています。



    VLAN のメンバーシップに関係なく、どの IP 要素（送信元 IP、送信先 IP、サービス種別など）でも任意の IP パケットを制御するアクセス ルールを作成できます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。

8. パケットに対する接続キャッシュ エントリが作成され、必要に応じて NAT 変換が実行されます。
9. TCP、VoIP、FTP、MSN、Oracle、RTSP のほか、メディア ストリーム、PPTP、およびL2TP に対するステートフル パケット検査および変換が実行されます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。
10. ゲートウェイ アンチウイルス、侵入防御、アンチスパイウェア、CFS、電子メール フィルタなどの精密パケット検査が実行されます。禁止されたパケットは破棄されてログに記録されます。許可されたパケットは引き続き処理されます。クライアント通知が設定どおりに実行されます。
11. パケットの宛先が暗号化ゾーン（VPN）、非保護ゾーン（WAN）、またはその他の接続インターフェース（非保護ゾーンとその他の接続インターフェースは、通常、混在モード トポロジの場合に該当）であった場合、パケットは適切なパスを介して送信されます。
12. パケットの宛先が VPN/WAN/接続インターフェースではなかった場合、保存されていた VLAN タグが復元され、（再び元の VLAN タグを持った）パケットが *ブリッジ パートナー* インターフェースへと送出されます。

L2 ブリッジ モードでの複数サブネット

「L2 ブリッジの IP パケット パス」の説明にあるように、L2 ブリッジ モードでは、ブリッジを介して任意の数のサブネットを処理できます。既定では、すべてのサブネットが許可されますが、アクセス ルールを適用してトラフィックを制御することも可能です。

L2 ブリッジ モードでの非 IPv4 トラフィック

サポート対象外のトラフィックは、既定では、L2 ブリッジ インターフェースからブリッジ パートナー インターフェースへと渡されます。これにより、装置は LLC パケット (Spanning Tree など) や他の EtherType (MPLS ラベル スイッチ パケット (EtherType 0x8847)、Appletalk (EtherType 0x809b)、Banyan Vines (EtherType 0xbad)) など、IPv4 以外のトラフィックを通過させることができます。これらの非 IPv4 パケットはブリッジを通過するだけで、パケット ハンドラによって検査されることも、制御されることもありません。これらのトラフィック タイプが不要である場合は、「**セカンダリ ブリッジ インターフェース**」設定ダイアログの「**すべての非 IPv4 トラフィックをブロックする**」オプションを有効にすることで、ブリッジの動作を変更できます。

L2 ブリッジ パスの決定

装置がブリッジ ペア インターフェースで受信したパケットは、適切かつ最適なパスに沿って送信先へと転送されなければなりません。そのパスはブリッジ パートナーである場合もあれば、その他の物理インターフェース (またはサブインターフェース) である場合もあります。あるいは VPN トンネルである場合も考えられます。同様に、ブリッジ ペア上の特定のホスト宛てに、他のパス (物理、仮想、または VPN) から到達したパケットは、適切なブリッジ ペア インターフェースを介して送出される必要があります。

以下は、こうした状況下で、パス決定に適用されるロジックを順に説明したものです。

1. 送信先に対して、既定以外の最も限定的なルートが存在する場合は、そのルートが選択されます。例えば、次のようなケースが該当します。
    a. ホスト `15.1.1.100` サブネット宛てのパケットが X3 (非 L2 ブリッジ LAN) に到達した。ここで、`15.1.1.0/24` サブネットへのルートが、X0 (セカンダリ ブリッジ インターフェース、LAN) インターフェースを介し、`192.168.0.254` を経由したパスに存在する。この場合、パケットは、X0 を介して、送信先IP アドレス `15.1.1.100` を持つ、`192.168.0.254` の送信先 MAC アドレスに転送されます。
    b. ホスト `10.0.1.100` 宛てのパケットが X4 (プライマリ ブリッジ インターフェース、LAN) に到達した。ここで、`10.0.1.0/24` へのルートが、X5 (DMZ)インターフェースを介し、`192.168.10.50` を経由したパスに存在する。この場合、パケットは、X5 を介して、送信先IP アドレス `10.0.1.100` を持つ、`192.168.10.50` の送信先 MAC アドレスに転送されます。
2. 送信先への特定のルートが存在しない場合は、送信先 IP アドレスを調べるために、ARP キャッシュ調査が実行されます。キャッシュ エントリと比較した結果、一致が見つかった場合、適切な送信先インターフェースが判明します。例えば、次のようなケースが該当します。
    a. ホスト `192.168.0.100` (L2プライマリ ブリッジ インターフェース X2 上に存在) 宛てのパケットが X3 (非 L2 ブリッジ LAN) に到着した。この場合、パケットは X2 を介し、ARP キャッシュから取得された既知の送信先 MAC および IP アドレス (`192.168.0.100`) に転送されます。
    b. X5 (DMZ) 上のホスト `10.0.1.10` 宛てのパケットが、X4 (プライマリ ブリッジ インターフェース、LAN) に到着した。この場合、パケットは X5 を介し、ARP キャッシュから取得された既知の送信先 MAC および IP アドレス (`10.0.1.10`) に転送されます。

3. ARP エントリが見つからない場合は、次の処理が行われます。
    a. パケットがブリッジ ペア インターフェースに到着した場合、そのパケットはブリッジ パートナー インターフェースに送信されます。
    b. パケットが他のパスから到着する場合、装置が、ブリッジ ペアの両方のインターフェースに ARP 要求を送出して、送信先 IP が存在するセグメントを特定します。

    最後のケースでは、ARP 応答を受信するまでは送信先が不明であるため、それまでは送信先ゾーンも判明しません。したがって、パスが決定するまで、装置は適切なアクセス ルールを適用できません。パスが決定された時点で、後続の関連するトラフィックに対して適切なアクセス ルールが適用されます。

L2 ブリッジ ペア インターフェースに到着したトラフィックのアドレス変換 (NAT) については、確定している送出先に応じて次のように処理されます。

1. ブリッジ パートナー インターフェースの場合、IP 変換 (NAT) は実行されません。
2. 異なるパスの場合は、そのパスに応じて適切な NAT ポリシーが適用されます。
    a. パスが別の接続 (ローカル) インターフェースである場合、変換が実行される可能性は低くなります。つまり、事実上、最終的な措置として、「**すべて > 元の NAT ポリシー**」に従ってルーティングされます。
    b. パスが WAN を経由することが確定している場合、既定の「*自動追加された [インターフェース] 発信 NAT ポリシー – X1 WAN*」が適用され、インターネットへの配信のためにパケットの送信元が変換されます。これは、「*内部セキュリティ*」で説明しているような混在モード トポロジの場合によく見られます。

L2 ブリッジ インターフェース ゾーンの選 択

ブリッジ ペア インターフェースのゾーンの割り当ては、実際のネットワークのトラフィック フロー要件に従って行う必要があります。トランスペアレント モードでは、送信元インターフェースをプライマリ WAN とし、トランスペアレント インターフェースを保護またはパブリックとすることで "高保護から低保護へと保護レベルが推移していくシステム" をある意味強制的に実現しています。これに対し、L2 ブリッジ モードでは保護の運用レベルをより細かく制御できます。例えば、L2 ブリッジ モードでは、プライマリ ブリッジ インターフェースとセカンダリ ブリッジ インターフェースを同じゾーンに割り当てることも、異なるゾーンに割り当てることもできます (LAN+LAN、LAN+DMZ、WAN+CustomLAN など)。こうした割り当ては、トラフィックに適用される既定のアクセス ルールだけでなく、ブリッジを通過するトラフィックに対する精密パケット検査セキュリティ サービスの適用方法にも影響します。ブリッジ ペアで使用するインターフェースを選択して構成する際、考慮すべき重要な要素として、セキュリティ サービス、アクセス ルール、および WAN 接続があります。

セキュリティ サービスの方 向 性

L2 ブリッジ モードを中心とした配備では、ブリッジ ペア インターフェースに対するゾーンを適切に選択するために、セキュリティ サービスの適用性を理解することが大切です。セキュリティ サービスの適用性は、次のような基準に基づいて決定されます。

1. **サービスの方向**:
    - GAV は、主にインバウンド サービスです。HTTP、FTP、IMAP、SMTP、POP3、TCPのインバウンド ストリームが検査されます。SMTP についてはアウトバウンド要素もあります。
    - アンチスパイウェア は、主にインバウンドです。インバウンドの HTTP、FTP、IMAP、SMTP、POP3 が検査され、通常はクラス ID によって識別されたスパイウェア コンポーネントの配信 (取得など) の有無がチェックされます。これとは別にアウトバウンド コンポーネントも存在します。スパイウェア コンポーネントの認識をトリガーする IPS シグネチャに固有の方向性 (すなわち"送信") と対比して、

ここでは“アウトバウンド”という用語を用いています。通常、これらのコンポーネントは、インターネット上のウェブ サーバ (WAN ホスト) から、クライアント (LAN ホストなど) によって HTTP 経由で取得されるため、送信の分類基準 (「IPS: トラフィックの方向」を参照) が使用されます。「IPS: トラフィックの方向」でいうと、これは送信接続に該当し、送信方向に分類されるシグネチャが必要となります。

- IPS には、受信、送信、両方向の 3 つの方向があります。受信と送信については「IPS: トラフィックの方向」に説明したとおりです。両方向とは、表において交差するすべてのポイントを指します。
- 精度を高めるため、接続状態 (SYN または確立済みなど) やフローにおけるパケットの送信元 (始動者または応答者など)、他の要素も考慮されます。

2. **トラフィックの方向**: IPS に関連したトラフィックの方向は、主にトラフィック フローの送信元および送信先ゾーンによって決まります。通常、装置がパケットを受信すると、そのパケットの送信元ゾーンが即座に判明し、その送信先ゾーンも、ルート (または VPN) 調査を実行することによってすぐに判別されます。

   パケットの方向性は、その送信元と送信先に基づき、受信と送信 (インバウンド/アウトバウンドと混同しないようにしてください) のいずれかに分類されます。この決定には、「IPS: トラフィックの方向 」に示す基準が使用されます。

   IPS: トラフィックの方向

送信先/送信元	非保護	公開	無線	暗号化	保護	マルチキャスト
非保護	受信	受信	受信	受信	受信	受信
公開	送信	送信	送信	受信	受信	受信
無線	送信	送信	信頼	信頼	信頼	受信
暗号化	送信	送信	信頼	信頼	信頼	送信
保護	送信	送信	信頼	信頼	信頼	送信

   表のデータは変更される場合があります。

   この分類に加えて、あるゾーンから別のゾーンへと、より高い信頼性を持って転送されるパケットは、本質的に高レベルのセキュリティ (LAN | 無線 | 暗号化 <--> LAN | 無線 | 暗号化) が確保されていることを表す、特別な信頼という種別に分類されます。信頼として分類されたトラフィックには、すべてのシグネチャが適用されます (受信、送信、および両方向)。

3. **シグネチャの方向**: これは、主に IPS に関連したものです。各シグネチャには、SonicWall のシグネチャ開発チームにより方向が割り当てられます。これは、擬陽性を最小限に抑えるための最適化措置として行われます。シグネチャには、次の方向があります。

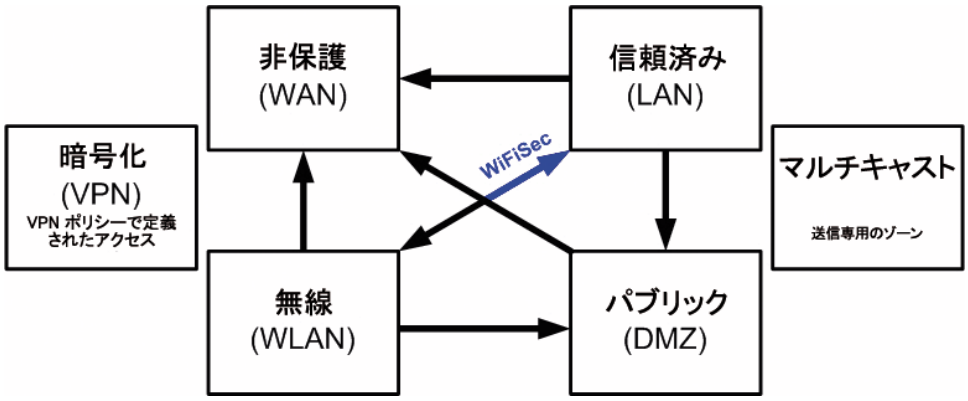
   - **受信** – 受信および信頼に適用されます。シグネチャの大半は受信です。これには、アプリケーションの脆弱性を狙ったあらゆる形態の攻撃のほか、列挙やフットプリンティングといった、あらゆる試みが含まれます。シグネチャの約 85%は受信です。
   - **送信** – 送信および信頼に適用されます。送信に分類されるシグネチャの例としては、IM や P2P のログイン試行のほか、悪性の応答 (例: 攻撃の応答) などがあります。シグネチャの約 10%は送信です。
   - **両方向** – すべてに適用されます。例えば、両方向のシグネチャには、IM ファイル転送、各種 NetBIOS 攻撃 (例: Sasser の通信)、各種 DoS 攻撃 (例: ポート 0 宛ての UDP/TCPトラフィック) があります。シグネチャの約 5%は両方向です。

4. **ゾーンの適用**: シグネチャがトリガーされるためには、必要なセキュリティ サービスが、*経路上のゾーンの少なくとも 1 つで有効になっている必要があります*。例えば、インターネット (X1、WAN) 上のホストが Microsoft ターミナル サーバ (X3、セカンダリ ブリッジ インターフェース、LAN) にアクセスしている場合、IPS が WAN、LAN、またはその両方で有効になっていれば、受信のシグネチャである “IPS 検出警告: MISC MS ターミナル サーバ要求、SID: 436、優先順位: 低” がトリガーされます。

既定のアクセス ルール

既定では、ゾーン対ゾーンのアクセス ルールが使用されます。必要に応じて変更することもできますが、既定のアクセス ルールをお勧めします。既定の設定を「」に示します。「既定のアクセス ルール」:

既定のアクセス ルール



WAN 接続

ライセンス、セキュリティ サービスに使用するシグネチャのダウンロード、NTP (時刻の同期)、CFS (コンテンツ フィルタ サービス) などのスタック通信には、インターネット (WAN) 接続が必要です。現時点では、これらの通信は、プライマリ WANインターフェース経由でしか行うことができません。これらのタイプの通信が必要な場合、プライマリ WANにインターネットへのパスが必要です。プライマリ WAN がブリッジ ペアに属しているかどうかは、これらのスタック通信を提供する機能に影響しません。

ⓘ **補足:** インターネット接続が利用できない場合、ライセンシングやシグネチャの更新を手動で実行することもできます。詳細については、https://www.MySonicWall.com/ を参照してください。

サンプル トポロジ

次の図は、一般的な配備を表すサンプル トポロジです。

- **インライン レイヤ 2 ブリッジ モード**では、SonicWall セキュリティ装置が追加されて、既に装置が備わっているネットワークでセキュリティ サービスを提供します。
- **境界セキュリティ**では、SonicWall セキュリティ装置がピュア L2 ブリッジ モードで既存のネットワークに追加されており、装置はネットワークの境界付近に配置されています。
- **内部セキュリティ**では、SonicWall セキュリティ装置が混在モードで完全統合されており、L2 ブリッジ、WLAN サービス、および NAT 変換による WAN アクセスを同時に提供します。
- **高可用性を備えたレイヤ 2 ブリッジ モード**は、装置の HA ペアが L2 ブリッジと共に高可用性を提供する混在モード シナリオを表しています。
- **SSL VPN を備えたレイヤ 2 ブリッジ モード**は、SonicWall SMA SSL VPN または SonicWall SSL VPN シリーズ装置が L2 ブリッジ モードと組み合わせて配備されているシナリオを表しています。

トピック:

- 無線レイヤ 2 ブリッジ
- インライン レイヤ 2 ブリッジ モード
- 境界セキュリティ
- 内部セキュリティ
- 高可用性を備えたレイヤ 2 ブリッジ モード
- SSL VPN を備えたレイヤ 2 ブリッジ モード

無線レイヤ 2 ブリッジ

ⓘ | **補足:** 無線レイヤ 2 ブリッジは、SuperMassive 9800 には適用されません。

無線モードでは、無線 (WLAN) インターフェースの LAN または DMZ ゾーンへのブリッジ後、WLAN ゾーンがセカンダリ ブリッジ インターフェースになり、無線クライアントが同等の有線クライアントと同じサブネットおよび DHCP プールを共有できるようになります。

WLAN から LAN へのレイヤ 2 インターフェース ブリッジを設定するには、次の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. ブリッジの対象とする無線インターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

   ⓘ | **ヒント:** 設定済みの仮想アクセス ポイントがある場合、既に WLAN ゾーン内の X4 などのインターフェースに VLAN インターフェースがあり、仮想アクセス ポイントはその VLAN ID を使用するように設定されています。
3. 「**レイヤ 2 ブリッジ モード**」で、「**モード/IP 割り当て**」を選択します。

   ⓘ | **補足:** WLAN ゾーンと選択したブリッジ インターフェースとの間のトラフィックを許可する一般的なルールが自動的に作成されますが、WLAN ゾーン タイプのセキュリティ ポリシーが依然として適用されます。限定的なルールがあれば手動で追加する必要があります。
4. WLAN のブリッジ先となるインターフェースを「**ブリッジ先**」から選択します。この例では、X0 (既定の LAN ゾーン) を選択します。
5. 残りのオプションは通常どおりに設定します。WLAN インターフェースの設定方法については、「無線インターフェースの設定」を参照してください。

インライン レイヤ 2 ブリッジ モード

この方式は、既に装置が備わっているネットワークで、ネットワークに大きな変更を加えずに装置のセキュリティ サービスを利用したいという場合に便利です。装置をレイヤ 2 ブリッジ モードで使用することにより、X0 および X1 インターフェースが同じブロードキャスト ドメイン/ネットワーク (X1 WAN インターフェース) の一部になります。

この例は、Hewlett Packard ProCurve スイッチング環境にインストールされた装置を表しています。SonicWall は HP の ProCurve Alliance のメンバーです。詳細は https://www.hpe.com/us/en/networking.html を参照してください。

HP の ProCurve Manager Plus (PCM+) および HP Network Immunity Manager (NIM) サーバ ソフトウェア パッケージを使用すると、装置の諸機能やスイッチを管理できます。

インライン レイヤ 2 ブリッジ モードを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. **X0 (LAN)** インターフェースの**設定**アイコンを選択します。

3. 「**インターフェースの編集**」ダイアログで、「IP 割り当て」を「**レイヤ 2 ブリッジ モード (IP ルート オプション)**」に設定します。オプションが次のように変化します。
4. 「**ブリッジ先:**」インターフェースを「**X1**」に設定します。
5. ブリッジ ペアですべての非 IP トラフィックを遮断するには、「**すべての非 IP トラフィックを遮断する**」を選択します。このオプションは、既定では選択されていません。
6. トラフィックがブリッジ ペアでルーティングされないようにするには、「**このブリッジ ペアにトラフィックをルーティングしない**」を選択します。このオプションは、既定では選択されていません。
7. ブリッジ ペアでトラフィックのスニッフのみを行う場合は、「**このブリッジ ペアのトラフィックのみスニフする**」を選択します。このオプションは、既定では選択されていません。
8. ブリッジ ペアでステートフル検査が行われないようにするには、「**このブリッジ ペアでステートフル インスペクションを無効にする**」を選択します。このオプションは、既定では選択されていません。
9. インターフェースが **HTTPS** および **SNMP** 用に設定されていて、**PCM+/NIM** で DMZ から管理できるようになっていることを確認します。
10. 残りのオプションは通常どおりに設定します。
11. 「**OK**」を選択すると、変更内容が保存されて有効になります。

LAN から WAN へのトラフィックおよび WAN から LAN へのトラフィックが許可されるようにアクセス ルールを変更することも必要です。そうしないと、トラフィックがうまく通りません。DMZ 上に PCM+/NIM サーバがある場合は、ファイアウォール上でルーティング情報に変更を加える必要もあるかもしれません。

境界セキュリティ

境界セキュリティは、セキュリティ サービス提供のために、装置を境界部分に追加したネットワーク シナリオです (装置とルータ間には既存の装置があってもなくてもかまいません)。通常、このシナリオでは、装置の下にあるものすべて (プライマリ ブリッジ インターフェース セグメント) は、装置の左側にあるものすべて (セカンダリ ブリッジ インターフェース セグメント) と比べて信頼レベルが低いと考えることができます。そのため、X1 (プライマリ WAN) をプライマリ ブリッジ インターフェースとして使用するのが適切です。

セカンダリ ブリッジ インターフェース (LAN) に接続されたホストからのアウトバウンド トラフィックは、ファイアウォールを介して (L3 スイッチ上の VLAN インターフェースとルータを順に通過して) ゲートウェイへと出ていくことが許可されます。一方、プライマリ ブリッジ インターフェース (WAN) からのインバウンド トラフィックは既定では通過できません。

セカンダリ ブリッジ インターフェース (LAN) セグメントにメール サーバやウェブ サーバなどのパブリック サーバが存在する場合、特定の IP アドレスやサービスについて WAN から LAN へのトラフィックを許可するアクセス ルールを追加すれば、これらのサーバへの受信トラフィックを許可することができます。

内部セキュリティ

装置が境界セキュリティ機器およびセキュア ワイヤレス プラットフォームとして動作するネットワーク シナリオです。同時に、*ワークステーションまたはサーバのアドレスを再割り当てすることなく*、ワークステーション セグメントとサーバ セグメント間の L2 ブリッジ セキュリティが実現されています。

装置は、ブリッジおよびルーティング/NAT を同時に行うことができますが、この配備例は、それを象徴する典型的な部門間混在モード トポロジと言えます。*プライマリ ブリッジ インターフェース* (サーバ) セグメントと*セカンダリ ブリッジ インターフェース* (ワークステーション) セグメントとの間を行き来するトラフィックは、L2 ブリッジを通過します。

ブリッジ ペアの両方のインターフェースが保護 (LAN) ゾーンに割り当てられているため、次の原則が成り立ちます。

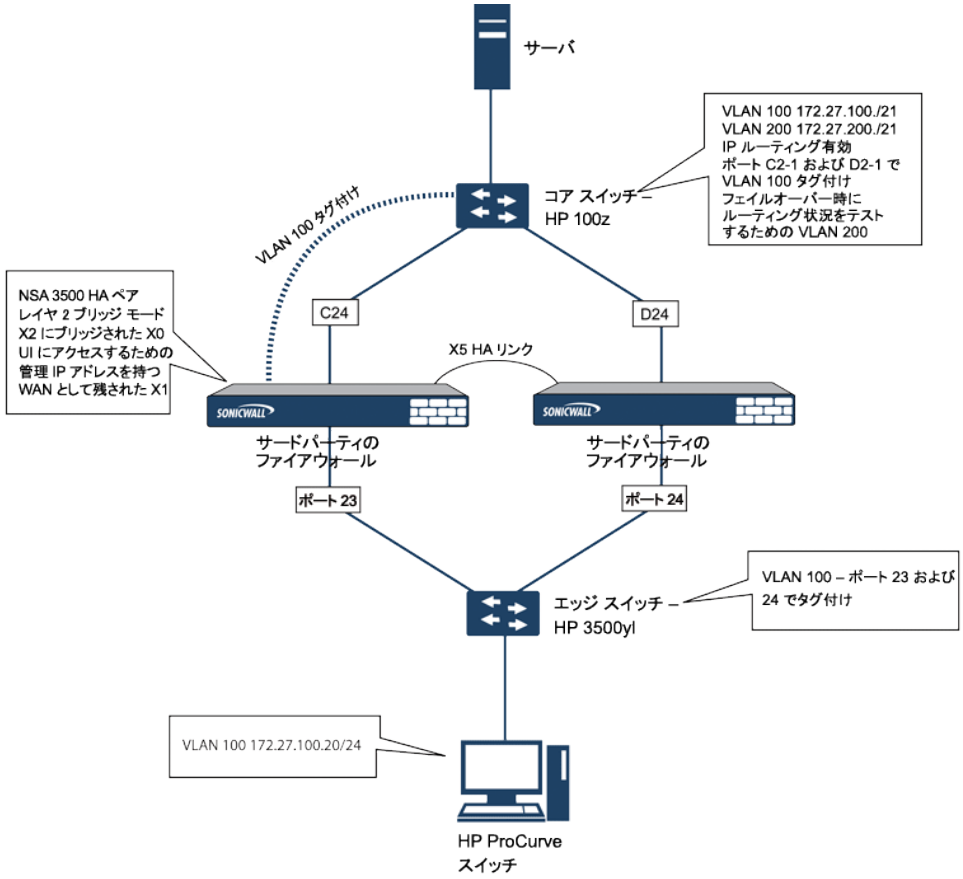
- 既定ではすべてのトラフィックが許可されます。ただし、必要に応じてアクセス ルールを作成することも可能です。
- 試しに、X2（プライマリ ブリッジ インターフェース）を公開（DMZ）ゾーンに割り当てたらどうなるかを考えてみます。この場合、すべてのワークステーションはサーバに到達することができますが、サーバからワークステーションへの通信を開始することはできません。これでトラフィック フローの要件が満たされる（ワークステーションからサーバへのセッションを開始するなど）場合もありますが、望ましくない影響が 2 点ほど生じます。
- DHCP サーバが DMZ に入ります。このため、ワークステーションからの DHCP 要求は L2 ブリッジを介して DHCP サーバ（192.168.0.100）に到達できますが、既定では DMZ から LAN へのアクセスがアクセス ルールによって拒否されるため、サーバからの DHCP OFFER は破棄されてしまいます。アクセス ルールを追加するか、既定のアクセス ルールを変更して、DMZ から LAN へのこのトラフィックを許可する必要があります。
- ワークステーションからサーバへのトラフィックは、送信元が保護ゾーンで送信先が公開ゾーンであるため、セキュリティ サービスの方向性は送信として分類されます。受信または（理想的には）信頼の分類に比べると、調査の水準が低くなるという点で、これは次善の選択肢と言えます。
- セキュリティ サービスの方向性は信頼として分類されます。また、すべてのシグネチャ（*受信*、*送信*、および*両方向*）が適用され、どちらのセグメントにも最高水準のセキュリティが提供されます。

レイヤ 2 ブリッジ モードでインターフェースを設定する詳細な手順については、「*レイヤ 2 ブリッジ モードの設定*」を参照してください。

高可用性を備えたレイヤ 2 ブリッジ モード

この方式は、高可用性（HA）とレイヤ 2 ブリッジ モードの両方が望まれるネットワークに適しています。この例は、装置の場合であり、VLAN を設定したスイッチの使用を想定しています。次を参照してください。「内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合」.

内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合



装置 HA ペアは、ポート X5（指定の HA ポート）で互いに接続された 2 つの装置から成っています。各装置のポート X1 は、通常の WAN 接続用に設定されており、その機器の管理インターフェースへのアクセスに使用されます。レイヤ 2 ブリッジ モードは、ポート X0 からポート X2 へのブリッジによって実装されています。

このシナリオを設定する際には、装置とスイッチの両方について注意すべき事柄がいくつかあります。

装置に関するもの

- 高可用性を設定するときに仮想 MAC オプションを有効にしないでください。レイヤ 2 ブリッジ モード設定では、この機能は有用ではありません。
- このようなインライン環境で先制モードを有効にするのはお勧めできません。先制モードが必要な場合は、スイッチのドキュメントに書かれている推奨事項に従ってください。ここではトリガとフェイルオーバーの時間値が重要な役割を果たすからです。
- 管理ネットワーク用のインターフェース（この例では X1 を使用）を確保することを検討してください。プローブやその他の理由でブリッジ インターフェースに IP アドレスを割り当てる必要がある場合、SonicWall ではセキュリティと管理のためにスイッチに割り当てた管理 VLAN ネットワークの使用を推奨しています。

ⓘ | **補足:** HA 用に割り当てた IP アドレスが実際のトラフィック フローと直接に相互作用することはありません。

スイッチに関するもの:

- 複数のタグ ポートの使用。「内部セキュリティの例: 高可用性とレイヤ 2 ブリッジ モードの両方が適切な場合」に示してあるように、エッジ スイッチ (ポート 23 および 24) とコア スイッチ (C24 — D24) の両方で VLAN 100 用に 2 つのタグ (802.1q) ポートが作成されています。この 2 つのスイッチの間で 装置がインラインで接続されています。高パフォーマンス環境では、リンク集約/ポート トランク、Dynamic LACP、またはこのような配備 (OSPF を使用) のために指定された完全に独立したリンクの使用が通常は推奨され、スイッチごとのフォールト トレランスを考慮する必要があります。詳細については、スイッチのドキュメントを参照してください。
- HP ProCurve スイッチでは、2 つのポートが同じ VLAN でタグ付けされた場合、そのポート グループは自動的にフェイルオーバー設定になります。その場合、一方のポートに障害が起きると、もう一方のポートがすぐに有効になります。

SSL VPN を備えたレイヤ 2 ブリッジ モード

このサンプル トポロジは、既存の SonicWall EX シリーズ SSL VPN または SonicWall SSL VPN ネットワーク環境への装置の適切なインストールに適用されます。装置をレイヤ 2 ブリッジ モードにすることにより、SSL VPN 装置への内部のプライベートな接続でウイルス、スパイウェア、および侵入を両方向でスキャンできます。このシナリオでは、装置がセキュリティを適用するためではなく、両方向のスキャン、ウィルスとスパムの遮断、および侵入の阻止に使用します。正しくプログラムすれば、トラフィックの動作や内容が有害であると判断されない限り、装置がネットワーク トラフィックを妨げることはありません。このセクションでは、装置の 1 ポート配備と 2 ポート配備の両方を取り扱います。

WAN から LAN へのアクセス ルール

この配備シナリオでは、装置をゲートウェイ アンチウイルス、アンチスパイウェア、および侵入防御の実施ポイントとしてのみ使用するので、既存のセキュリティ ポリシーを修正して、トラフィックが WAN と LAN の間を両方向に行き来できるようにする必要があります。

ネットワーク インターフェースの設定と L2B モードの有効化

このシナリオでは、WAN インターフェースを次の目的に使用します。

- 管理者用の管理インターフェースへのアクセス
- MySonicWall での購読サービスの更新
- 機器の既定のルートと SSL VPN 装置の内部トラフィックの「次のホップ」(そのため、WAN インターフェースは SSL VPN 装置の内部インターフェースと同じ IP セグメントにある必要があります)

装置の LAN インターフェースは、SSL VPN 装置の外部インターフェースから届く暗号化されていないクライアント トラフィックの監視に使用されます。このことは、(この LAN インターフェースを既定のルートと見なすために SSL VPN 装置の外部インターフェースを再構成する代わりに) レイヤ 2 ブリッジ モードで実行する理由になっています。

インターフェースで L2B モードを有効にするには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. WAN インターフェースの**設定**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 装置がシグネチャの更新を取得して NTP と通信できるように、インターネットにアクセスできるアドレスをインターフェースに割り当てます。ゲートウェイと内部/外部 DNS アドレスの設定は SSL VPN 装置の設定と一致している必要があります。

- **IP アドレス**: これは SSL VPN 装置の内部インターフェースのアドレスと一致しなければなりません。
- **サブネット マスク、デフォルト ゲートウェイ、DNS サーバ**: これらのアドレスを SSL VPN 装置の設定と一致させます。

4. 「**管理**」設定で、「**HTTPS**」および「**Ping**」を選択します。
5. 「**OK**」を選択すると、変更内容が保存されて有効になります。

LAN インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. LAN インターフェースの**設定**アイコンを選択します。
3. 「**ネットワーク モード**」設定として、「**レイヤ 2 ブリッジ モード**」を選択します。
4. 「**ブリッジ先**」設定として、「**X1**」を選択します。
5. 装置でサポートされている、VLAN タグ付きのトラフィックを通過させる必要もある場合は、「**VLAN フィルタリング**」を選択します。
6. 通過させる必要のある VLAN をすべて追加します。
7. 「**OK**」を選択すると、変更内容が保存されて有効になります。

装置の管理インターフェースから自動的に切断されることもあります。ここで装置の X0 インターフェースから管理用のラップトップまたはデスクトップを切断し、ネットワークに物理的に接続する前に装置の電源を切ることができます。

ネットワークと SSL VPN 装置の間への装置のインストール

配備方式（シングルホームまたはデュアルホーム）に関係なく、装置を SSL VPN 装置の X0/LAN インターフェースと内部ネットワークへの接続との間に配置する必要があります。そうすることで、機器が SonicWall のライセンスおよびシグネチャの更新サーバに接続したり、内部ネットワーク リソースへのアクセスを要求する外部クライアントからの復号化されたトラフィックをスキャンしたりすることが可能になります。

SSL VPN 装置がサードパーティのファイアウォールの背後にあって 2 ポート モードの場合、それはデュアルホームです。

デュアルホーム SSL VPN 装置を接続するには、次の手順に従います。

1. 装置の X0/LAN ポートを SSL VPN 装置の X0/LAN ポートにケーブルで接続します。
2. 装置の X1/WAN ポートを、SSL VPN を前に接続したポートにケーブルで接続します。
3. 装置の電源を入れます。

SSL VPN 装置がサードパーティのファイアウォールの DMZ 内にあって 1 ポート モードの場合、それはシングルホームです。

シングルホーム SSL VPN 装置を接続するには、次の手順に従います。

1. 装置の X0/LAN ポートを SSL VPN 装置の X0/LAN ポートにケーブルで接続します。
2. 装置の X1/WAN ポートを、SSL VPN を前に接続したポートにケーブルで接続します。
3. 装置の電源を入れます。

設定の構成または確認

この段階で、ネットワーク内の管理ステーションから装置の管理インターフェースに WAN IP アドレスを使ってアクセスできるようになっているはずです。

設定を構成または確認するには、以下の手順に従います。

1. 装置のすべてのセキュリティ サービスが有効になっていることを確認します。「*サービスのライセンス取得*」と「*ゾーンごとのセキュリティ サービスの有効化*」を参照してください。
2. 機器を SonicWall SMA SSL VPN 装置と共に配備する前に、SonicWall コンテンツ フィルタ サービスを無効にする必要があります。
    a. 「**オブジェクト | 一致オブジェクト > ゾーン**」ページに移動します。
    b. 「**LAN (X0)**」ゾーンの横にある「**設定**」を選択します。
    c. 「**コンテンツ フィルタ サービスを強制する**」を無効にします。
    d. 「**OK**」を選択します。
3. 装置での管理者パスワードをまだ変更していなければ、「**デバイス | 設定 > 管理**」で変更することができます。
4. 外部クライアントからのネットワークへのアクセスをテストするには、SSL VPN 装置に接続し、ログインします。
5. 接続したら、内部ネットワーク リソースへのアクセスを試みます。何か問題があれば、設定を確認し、「*レイヤ 2 ブリッジ モード配備における一般的な項目の設定*」を参照してください。

レイヤ 2 ブリッジ モードの設定

トピック:

- レイヤ 2 ブリッジ モード用の設定タスク リスト
- レイヤ 2 ブリッジ モード手順の設定
- レイヤ 2 ブリッジ モードでの VLAN 統合
- レイヤ 2 ブリッジ モードでの VPN 統合

レイヤ 2 ブリッジ モード用の設定タスク リスト

- ネットワークに合ったトポロジを選択します。
- レイヤ 2 ブリッジ モード配備における一般的な項目の設定
    - セキュリティ サービスをライセンスします。
    - DHCP サーバを無効化します。
    - SNMP および HTTP/HTTPS 管理を設定し有効化します。
    - Syslog を有効化します。
    - 対象ゾーンに関してセキュリティ サービスを有効化します。
    - アクセス ルールの作成
    - ログ設定
    - 無線ゾーンを設定します。
    - 無線ゾーンの設定は、SuperMassive 9800 には適用されません。
- プライマリ ブリッジ インターフェースの設定
    - プライマリ ブリッジ インターフェースのゾーンを選択します。
    - 管理を有効化します。
    - セキュリティ サービスを有効化します。

- セカンダリ ブリッジ インターフェースの設定
    - セカンダリ ブリッジ インターフェースのゾーンを選択します。
    - 管理を有効化します。
    - セキュリティ サービスを有効化します。
- 適切なゾーンにセキュリティ サービスを適用します。

レイヤ 2 ブリッジ モード配備における一般的な項目の設定

大部分のレイヤ 2 ブリッジ モード トポロジでは、装置の使用に先だって次の設定を行う必要があります。

- サービスのライセンス取得
- DHCP サーバの無効化
- SNMP の設定
- インターフェースの SNMP および HTTPS の有効化
- Syslog の有効化
- ゾーンごとのセキュリティ サービスの有効化
- アクセス ルールの作成
- ログの設定
- 無線ゾーンの設定

サービスのライセンス取得

装置が正しく登録されている場合、以下の手順に従います。

1. 「**デバイス | 設定 > ライセンス**」に移動します。
2. 「**セキュリティ サービスのオンライン管理**」の下にある「**同期**」を選択します。

これにより、装置ライセンス サーバへの接続が行われ、装置が確実にライセンスを受けられるようになります。

ライセンス状況を確認するには、「**デバイス | 設定 > 状況**」ページに移動し、すべてのセキュリティ サービス（ゲートウェイ アンチウイルス、アンチスパイウェア、侵入防御）のライセンス状況を表示します。

DHCP サーバの無効化

別の機器が DHCP サーバとして動作しているネットワーク設定で装置をレイヤ 2 ブリッジ モードで使用するときは、まず装置の内部の DHCP エンジンを無効にする必要があります。既定では、このエンジンが設定されて動作しています。

DHCP サーバを無効にするには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ**」に移動します。
2. 「**DHCP サーバを有効にする**」を無効にします。
3. 「**適用**」を選択します。

SNMP の設定

SNMP の設定を行うには、以下の手順に従います。

1. 「**デバイス | 設定 > SNMP**」に移動します。
2. 「**SNMP を有効にする**」を選択します。

3. 「**適用**」を選択します。「設定」が使用可能になり、SNMP 情報が設定されます。
4. 「**設定**」を選択します。「**SNMP の設定**」ダイアログが表示されます。SNMP の設定方法については、「*SNMP アクセスの設定*」を参照してください。

インターフェースの SNMP および HTTPS の有効化

インターフェースで SNMP および HTTPS を有効化するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 装置の管理に使用するインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**管理**」オプションとして、**HTTPS** および **SNMP** を有効化します。
4. 「**OK**」を選択します。

Syslog の有効化

「**デバイス | ログ > Syslog**」ページで Syslog を有効にします。Syslog を有効にする方法については、『*SonicOS ログ管理ガイド*』を参照してください。

ゾーンごとのセキュリティ サービスの有効化

「**ネットワーク | システム > インターフェース**」で、使用するゾーンごとにセキュリティ サービスが有効になっていることを確認します。

次に「**ポリシー | セキュリティ サービス**」で、サービスごとに、環境に最も適した設定項目を有効にして設定します。セキュリティ サービスの有効化と設定については、『*SonicOS セキュリティ サービス管理ガイド*』を参照してください。

アクセス ルールの作成

異なるゾーンの装置を管理したり、あるいはサードパーティのサーバを管理、SNMP、Syslog サービスで使用したりする場合は、ゾーン間のトラフィックに関してアクセス ルールを作成します。「**ポリシー | ルールとポリシー > アクセス ルール**」で、そのサーバのゾーンとユーザおよびサーバが含まれるゾーンとの共通部分のアイコンを選択します（環境によっては共通部分が複数存在することもあります）。新しいルールを作成して、サーバがそのゾーンのすべての機器と通信できるようにします。アクセス ルールについては、『*SonicOS ポリシー管理ガイド*』を参照してください。

ログの設定

「**デバイス | ログ > 名前解決**」で、「**名前解決方法**」を「**DNS の後に NetBIOS**」に設定します。ログの設定については、『**SonicOS ログ管理ガイド**』を参照してください。

無線ゾーンの設定

HP PCM+/NIM システムを使用して、WLAN/無線ゾーンに割り当てたインターフェース上の HP ProCurve スイッチを管理するのであれば、2 つの機能を無効にする必要があります。そうしないと、スイッチを管理できません。

無線ゾーンを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 無線ゾーンを選択します。

3. 「無線」で、「**SonicPoint により生成された通信のみ許可する**」および「WiFiSec 強制」オプションを無効にします。
4. 「**OK**」を選択します。

レイヤ 2 ブリッジ モード手順の設定

ご使用のネットワークに最適なトポロジの選択については、「L2 ブリッジ インターフェース ゾーンの選択」を参照してください。この例では、「単純な L2 ブリッジ トポロジ」に最も近いトポロジを使用します。

プライマリ ブリッジ インターフェースとして使用するインターフェースを選択します。詳細については、「L2 ブリッジ インターフェース ゾーンの選択」を参照してください。この例では、(プライマリ WAN に自動的に割り当てられる) X1 を使用します。

トピック:

- プライマリ ブリッジ インターフェースの設定
- セカンダリ ブリッジ インターフェースの設定
- ハードウェア障害に備えた L2 バイパスの設定

プライマリ ブリッジ インターフェースの設定

プライマリ ブリッジ インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. X1 (WAN) インターフェースの右の列で**設定**アイコンを選択します。
3. インターフェースに静的 IP アドレス (`192.168.0.12` など) を設定します。

   ⓘ | **補足:** プライマリ ブリッジ インターフェースには、静的 IP を割り当てる必要があります。
4. WAN インターフェースの場合のみ:
   a. デフォルト ゲートウェイを設定します。これは、装置そのものをインターネットに到達させるための必須の設定です。
   b. DNS サーバを設定します
5. インターフェースに対する「**管理**」オプションを 1 つ以上選択します。**HTTPS**、**Ping** (既定で選択されている)、**SNMP**、**SSH**。

   ⓘ | **補足:** 「**HTTPS**」を選択すると、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」が自動的に選択されます。HTTP/HTTPS リダイレクトの詳細は、「HTTP/HTTPS リダイレクト」を参照してください。
6. 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。
7. HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト」を参照してください。
8. 「**OK**」を選択します。

セカンダリ ブリッジ インターフェースとして使用するインターフェースを選択します。詳細については、「L2 ブリッジ インターフェース ゾーンの選択」を参照してください。

セカンダリ ブリッジ インターフェースの設定

この例では、(LAN に自動的に割り当てられる) X0 を使用します。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. X0(LAN) インターフェースの右の列で「**設定**」アイコンを選択します。
3. 「**ネットワーク モード**」で、「**レイヤ 2 ブリッジ モード**」を選択します。
4. 「**ブリッジ先**」で、「**X1**」インターフェースを選択します。
5. インターフェースに対する「**管理**」オプションを 1 つ以上選択します。**HTTPS**、**Ping** (既定で選択されている)、**SNMP**、**SSH**。

   ⓘ **補足:** 「HTTPS」を選択すると、「HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する」が自動的に選択されます。HTTP/HTTPS リダイレクトの詳細は、「HTTP/HTTPS リダイレクト」を参照してください。
6. 「**ユーザ ログイン**」オプションを選択します。**HTTP** と **HTTPS** のいずれか、または両方のプロトコルを選択します。
7. HTTP から HTTPS へのリダイレクトを有効にするには、「**HTTP から HTTPS へのリダイレクトを有効にするためのルールを追加する**」を選択します。このオプションの詳細については、「HTTP/HTTPS リダイレクト」を参照してください。
8. 必要に応じて、L2 ブリッジが IPv4 以外のトラフィックを通すことを防ぐために「**すべての非 IPv4 トラフィックを遮断する**」を有効にすることもできます。
9. L2 ブリッジを通る VLAN トラフィックを制御するには、「**VLAN フィルタ**」を選択します。既定では、すべての VLAN が許可されます。
   - ドロップダウン リストから「**リストされた VLAN を遮断する (ブラックリスト)**」を選択し、遮断する VLAN を左ペインから選んで右ペインに追加します。右ペインに追加された VLAN はすべて遮断されます。また、左ペインに残っている VLAN はすべて許可されます。
   - ドロップダウン リストから「**リストされた VLAN を許可する (ホワイトリスト)**」を選択し、明示的に許可する VLAN を左ペインから選んで右ペインに追加します。右ペインに追加された VLAN はすべて許可されます。また、左ペインに残っている VLAN はすべて遮断されます。
10. 「**OK**」を選択します。「**インターフェース設定**」テーブルに更新された設定が表示されます。

これで、必要に応じて、セキュリティ サービスを適切なゾーンに適用できるようになりました。この例では、LAN、WAN、または両方のゾーンにセキュリティ サービスを適用する必要があります。

ハードウェア障害に備えた L2 バイパスの設定

L2 バイパスを使用すると、インターフェースが LAN バイパス機能を持つ別のインターフェースにブリッジされる際に、装置の物理的バイパスを行うことができます。これにより、回復不能なファイアウォールの障害が発生した場合も、ネットワーク トラフィックが流れ続けることができます。

L2 バイパス リレーが閉じられると、バイパスされたインターフェース (X0 および X1) に接続されたネットワーク ケーブルは、単一の連続的なネットワーク ケーブルのように物理的に接続されます。「**異常時の物理的なバイパスを保証する**」オプションを有効にすると、異常時にファイアウォールをバイパスすることにより、ネットワーク トラフィックの中断を回避できます。

L2 バイパスは、**レイヤ 2 ブリッジ モード**のインターフェースにのみ設定できます。「**異常時の物理的なバイパスを保証する**」オプションは、「**モード / IP 割り当て**」で「**レイヤ 2 ブリッジ モード**」を選択した場合のみ表示されます。ブリッジペアの 2 つのインターフェースの間に物理的なバイパス リレーがないかぎり、このオプションは表示されません。

「**異常時の物理的なバイパスを保証する**」オプションを有効にすると、他の「**レイヤ 2 ブリッジ モード**」オプションも自動的に次のように設定されます。

- **すべての非 IPv4 トラフィックを遮断する** – 無効。このオプションが有効の場合、すべての非 IPv4 イーサネット フレームが遮断されます。そのため、このオプションは無効になります。

- **このブリッジ ペアにトラフィックをルーティングしない** – 有効。このオプションが有効の場合、ブリッジ ペアのピア ネットワーク以外に向けてパケットがルーティングされるのを防ぎます。そのため、このオプションは有効になります。
- **このブリッジ ペアのトラフィックのみスニフする** – 無効。このオプションが有効の場合、ブリッジ ペアのインターフェースで受信したトラフィックは一切転送されません。そのため、このオプションは無効になります。
- **このブリッジ ペアでステートフル インスペクションを無効にする** – 変更しない。このオプションは影響を受けません。

L2 バイパスを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 設定するインターフェースの「**設定**」列にある**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**異常時の物理的なバイパスを保証する**」を選択します。

   ⓘ **補足:** 「**異常時の物理的なバイパスを保証する**」オプションは、NSA-6600 以降の装置で X0 および X1 インターフェースをブリッジしている場合にのみ利用可能です。
4. 「**OK**」を選択します。

レイヤ 2 ブリッジ モードでの VLAN 統合

VLAN は、SonicWall セキュリティ装置でサポートされています。VLAN タグを持ったパケットが物理インターフェースに到着すると、VLAN ID が評価され、それがサポートされているかどうかが判断されます。VLAN タグが除去され、その後は、他のトラフィックと同じようにパケット処理が続行されます。受信および送信パケット パスの単純化された表示には、繰り返しが起こり得る次の手順が含まれます。

- IP 検証と再組み立て
- カプセル化解除 (802.1q、PPP)
- 復号化
- 接続キャッシュの調査と管理
- ルート ポリシー調査
- NAT ポリシー調査
- アクセス ルール (ポリシー) 調査
- 帯域幅管理
- NAT 変換
- 高度なパケット処理 (該当する場合)
  - TCP 検証
  - 管理トラフィック処理
  - コンテンツ フィルタ
  - 変換とフロー分析 (SonicWall セキュリティ装置の場合): H.323、SIP、RTSP、ILS/LDAP、FTP、Oracle、NetBIOS、Real Audio、TFTP
  - IPSおよびGAV

この時点で、許可されたトラフィックであると確認された場合、そのパケットが送信先へと転送されます。パケットの送信パスには次の処理が含まれます。

- 暗号化
- カプセル化
- IP 断片化

送信時には、ルート ポリシーの調査によってゲートウェイ インターフェースが VLAN サブインターフェースであると判断された場合、パケットが適切な VLAN ID ヘッダーでタグ付け（カプセル化）されます。ファイアウォールのルーティング ポリシー テーブルは、VLAN サブインターフェースを作成すると自動的に更新されます。

VLAN サブインターフェースに関連した NAT ポリシーおよびアクセス ルールの自動作成は、物理インターフェースの場合とまったく同じように行われます。VLAN 間のトラフィックを制御するルールおよびポリシーは、SonicOS の使いやすく効率的なインターフェースを使ってカスタマイズできます。

一般的な管理の過程で、またはサブインターフェースの作成手順でゾーンを作成する際、ゾーンの作成ページに、そのゾーンに対する GroupVPN の自動作成を制御するチェックボックスが表示されます。既定では、新たに作成された無線タイプのゾーンについてのみ、「**GroupVPN を生成する**」が有効になっています。なお、このオプションは、他のゾーン タイプでもゾーンの作成時にチェックボックスをオンにすることで有効化できます。

VLAN サブインターフェース間のセキュリティ サービスの管理は、ゾーン レベルで行われます。すべてのセキュリティ サービスは、物理インターフェース、VLAN サブインターフェース、またはその両者の組み合わせから成るゾーンに対して設定および適用できます。

異なるワークグループ間の ゲートウェイ アンチウイルス および 侵入防御 は、保護セグメントごとに専用の物理インターフェースを用意しなくても、VLAN のセグメント化によって容易に達成できます。

VLAN サポートにより、組織は、ファイアウォール上で専用の物理インターフェースを使用することなく、各種ワークグループ間やワークグループとサーバ ファーム間に（単純なパケット フィルタと比べて）より効果的な内部セキュリティを導入できます。

本書では、VLAN サブインターフェースを WAN ゾーンに割り当てて、WAN クライアント モードを使用する機能（WAN ゾーンに割り当てられた VLAN サブインターフェースでは、静的アドレッシングのみサポートされます）のほか、WAN 負荷分散およびフェイルオーバーをサポートする機能を紹介しています。また、SonicPoint をワークグループ スイッチ上のアクセス モードの VLAN ポートに接続することによって、ネットワーク全体に SonicPoint を分散させる方法についても紹介しています。これらのスイッチは、コア スイッチにバックホールされ、その後、すべての VLAN がトランク リンクを介して装置に接続されます。

レイヤ 2 ブリッジ モードでの VPN 統合

レイヤ 2 ブリッジ モード向けにも設定されているインターフェースでの VPN 設定時には、受信 VPN トラフィックが適切に装置を通過するように追加のルートを設定する必要があります。

レイヤ 2 ブリッジ モードで VPN 統合を設定するには、以下の手順に従います。

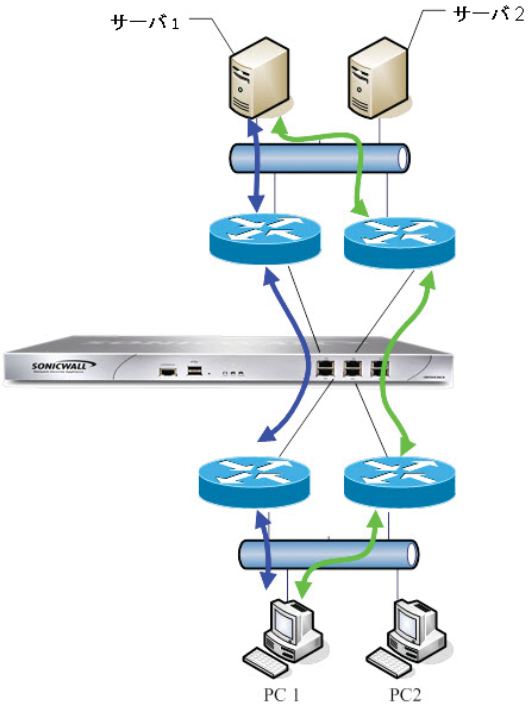
1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. **追加**アイコンを選択します。「**ルート ポリシーの追加**」ダイアログが表示されます。
3. ルートを次のように設定します。
   - 送信元: **すべて**
   - 送信先: *ユーザ定義の VPN アドレス オブジェクト*（これはローカル VPN トンネルの IP アドレス範囲を表すアドレス オブジェクトです）
   - サービス: **すべて**
   - ゲートウェイ: `0.0.0.0`
   - インターフェース: **X0**
4. 「**OK**」を選択します。

非対称ルーティング

SonicOS は非対称ルーティングをサポートしています。非対称ルーティングとは、往路と復路でパケットのフローが別のインターフェースを通るようなルーティングです。これが行われることがあるのは、トラフィックが装置上の異なるレイヤ 2 ブリッジ ペア インターフェースを通るとき、または高可用性クラスタ内の異なる装置を通るときです。

精密パケット検査またはステートフルなファイアウォール アクティビティを実行するすべての装置は、パケット フローに関連付けられているすべてのパケットを "確認" する必要があります。これは、フロー内の各パケットが、目的の送信先に到達する限り、理論的には異なるパスに沿って転送されてもよい (つまり、介在するルータがパケットをいちいち確認しなくてよい) 従来の IP ルーティングとは対照的です。現在のルータは各パケット フローで一貫したネクストホップによるパケット転送を試みますが、これは一方向へのパケット転送にしか当てはまりません。ルータは、送信側ルータへの戻りのトラフィックの誘導を一切試みません。こうした IP ルーティング動作は、非対称ルーティングをサポートしない装置クラスタにとって問題となります。一連のクラスタ ノードが、すべて同じネットワークへのパスを提供するからです。クラスタを介してネットワークにパケットを転送するルータは、任意のクラスタ ノードをネクストホップとして選択する可能性があります。その結果、ある方向へのパケットのフローに使用されたノードがその戻りのパスで使用されるノードとは異なる非対称なルーティングとなります。フローのこの変化が、一方または両方のクラスタ ノードでトラフィックが破棄される原因となります。どちらのノードもフローのすべてのトラフィックを "確認" していないからです。次を参照してください。「非対称ルーティング」.

非対称ルーティング



非対称ルーティング トラフィック

「「非対称ルーティング」」で、PC1 が Server1 と通信するとき、双方向のトラフィックは異なるルータを通ります。つまり、同じ接続のパケットの中に青色のパスを通るものと、緑色のパスを通るものがあります。このような配備では、ルータが冗長ルート プロトコルや負荷分散プロトコル (例えば、Cisco HSRP プロトコル) を実行することがあります。

SonicOS ではステートフル検査が使われます。この装置を通るすべての接続はインターフェースに関連付けられます。しかし、非対称ルーティングがサポートされるようになったので、SonicOS は、フローが異なるインターフェースを通るときも、受信トラフィックと送信トラフィックを追跡し、ステートフルな精密パケット検査を提供します。

ⓘ **補足:** 非対称ルーティングは、応答を返さない単方向接続（すなわち、TCP 状態バイパス）とは別のものです。

インターフェースの IPv6 設定

IPv6 インターフェースの設定の詳細については、「*IPv6 インターフェースの設定*」を参照してください。

31 ビット ネットワーク設定

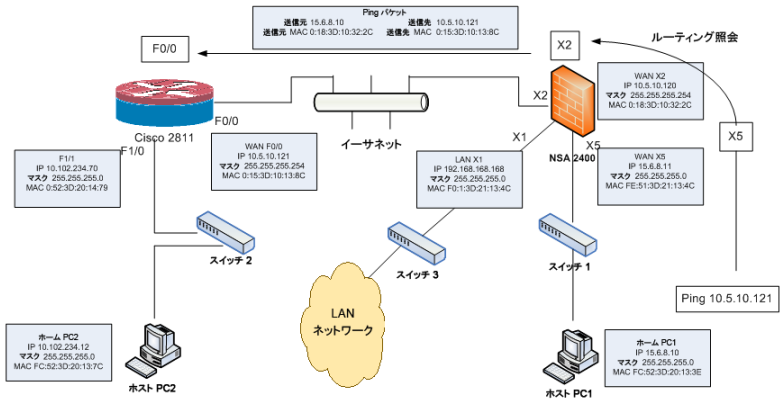
SonicOS では、31 ビットのサブネット マスクの使用を定義する RFC 3021 がサポートされるようになりました。このマスクでは、サブネット内で 2 つのホスト アドレスしか使用できず、ネットワーク アドレスやゲートウェイ アドレス、ブロードキャスト アドレスはありません。このような設定は、大規模なネットワーク内で 2 つのホストをポイント ツー ポイント リンクで接続するために使用できます。この変更がアドレス空間の節約に結び付くことは明白で、大規模なネットワーク内の各ポイント ツー ポイント リンクが消費するアドレスが 4 つではなく 2 つになります。

ここでいうポイント ツー ポイント リンクは、PPP (Point to Point Protocol) とは異なります。31 ビット マスクを使用するポイント ツー ポイント リンクでは、PPP プロトコルを使用してもしなくてもかまいません。ポイント ツー ポイント リンク上の 31 ビットの接頭辞付き IPv4 アドレスは、イーサネット ネットワークでも使用できます。

トピック:

- 31 ビット ネットワーク環境の例
- SonicOS での 31 ビット ネットワークの設定

31 ビット ネットワーク環境の例



このネットワーク環境では、ホスト PC1 とホスト PC2 は相互にアクセスすることができます。一方、LAN ネットワーク内のホストはホスト PC2 にアクセスすることができます。

この環境用の設定を行うには、以下の手順に従います。

1. ホスト PC1 で、次のように 2 つのルート エントリを追加します。
   - `Route add 10.5.10.0 mask 255.255.255.0 15.6.8.10`
   - `Route add 10.102.234.0 mask 255.255.255.0 15.6.8.10`
2. ホスト PC2 で、次のように 2 つのルート エントリを追加します。
   - `Route add 10.5.10.0 mask 255.255.255.0 10.102.234.70`
   - `Route add 15.6.8.0 mask 255.255.255.0 10.102.234.70`
3. Cisco ルータ (F0/0) で、次の設定を行います。
   - `interface fastEthernet 0/0`
   - `ip address 10.5.10.120 255.255.255.254`
4. Cisco 2811 で、次のように 1 つのルート エントリを追加します。

```
!
ip route 15.6.8.0 255.255.255.0 10.5.10.120
!
```

5. ファイアウォールで、次のように 1 つのルート エントリを追加して、WAN ゾーンのデータが X2 から X5、および X5 から X2 に流れるようにします。

```
Any 10.102.234.0 Any X2 Default Gateway X2
```

SonicOS での 31 ビット ネットワークの設定

SonicOS のインターフェースを 31 ビット サブネット用に設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 目的のインターフェースを編集します。
3. 「**サブネット マスク**」を `255.255.255.254` に設定します。
4. 「**IP アドレス**」フィールドに一方のホスト IP アドレスを入力します。
5. 「**デフォルト ゲートウェイ**」フィールドにもう一方のホスト IP アドレスを入力します。
6. 必要に応じて、使用中のネットワークに合わせて他のフィールドを設定します。
7. 「**OK**」を選択します。

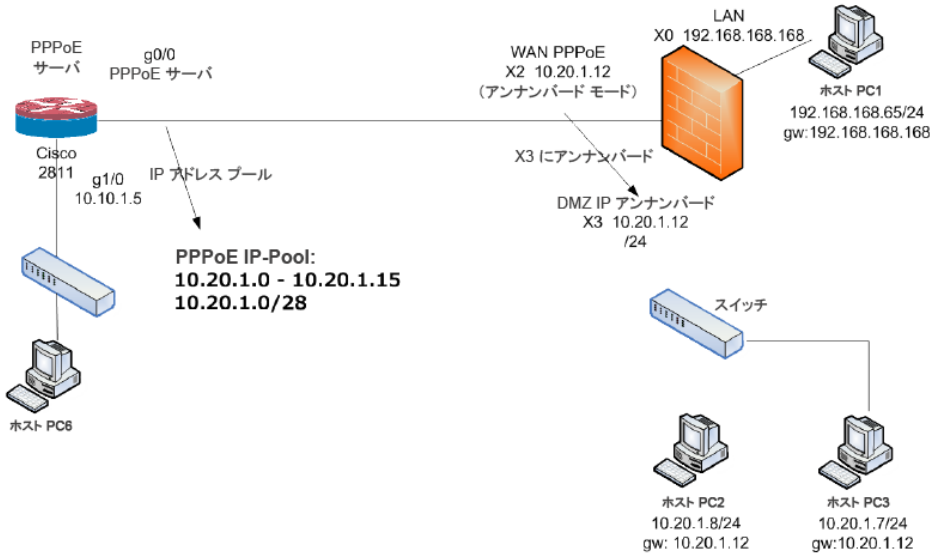
PPPoE アンナンバード インターフェースのサポート

PPPoE アンナンバード インターフェースを使用すると、1 つの PPPoE 接続で一連の IP アドレスを管理できます。インターネット サービス プロバイダ (ISP) は、サブネット内で割り当て可能な複数の静的 IP アドレスを提供します。最初のアドレスはネットワーク アドレスとして指定され、最後のアドレスはブロードキャスト アドレスとして指定されます。

PPPoE の既定の MTU は **1492** です。

トピック:

サンプル ネットワークトポロジ



このトポロジでは、X2 は PPPoE アンナンバード インターフェースで、X3 はアンナンバード インターフェースです。

SonicOS は、2 つのポリシーを「**ネットワーク | システム > 動的ルーティング**」テーブルに追加します。

SonicOS は 2 つの NAT ポリシーも追加します。

注意

X2 から X3 へのアンナンバードが設定されているときに、X3 を別のモードに変更するには、先に X2 を別のモードに変更して X2 との関係を終了します。そうしないと、インターフェース X3 の IP アドレスまたはマスクを変更した場合に、X3 は PPPoE サーバに再接続します。

X3 がアンナンバード インターフェースとして設定されている場合、他のインターフェースから L2 ブリッジを使用して X3 に接続することはできません。

PPPoE アンナンバード インターフェースの設定

PPPoE アンナンバード インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. **編集**アイコンを選択して、WAN インターフェースに対する PPPoE クライアント設定を行います。「**インターフェースの編集**」ダイアログが表示されます。
3. 「**アンナンバード インターフェース**」を選択します。ドロップダウン メニューがアクティブになります。
4. 「**新規アンナンバード インターフェースの作成**」を選択します。「**アンナンバード インターフェースの追加**」ダイアログが表示されます。
5. 「**ゾーン**」で、「**LAN**」または「**DMZ**」を選択するか、新しいゾーンを作成します。

ⓘ | **補足:** 「**モード / IP 割り当て**」が「**IP アンナンバード**」に設定され、淡色表示になります。

6. 「**IP アドレス**」には、ISP から提供されたアドレスを入力します。通常は、プロバイダから割り当てられた 2 番目の IP アドレスを使用します。
7. 「**サブネット マスク**」フィールドに、ISP によって割り当てられたサブネット マスクを入力します。
8. このインターフェースの設定を終了します。
9. 「**OK**」を選択します。
10. 最初のインターフェースの設定を終了します。
11. 「**OK**」を選択します。

PPPoE アンナンバードによる HA の設定

PPPoE アンナンバードによる高可用性機能 (HA) の設定方法については、「*アクティブ/スタンバイ高可用性機能の設定*」を参照してください。

2

フェイルオーバーと負荷分散

WAN フェイルオーバーによって、ユーザ定義インターフェースの 1 つをバックアップ WAN ポートとして設定できます。バックアップ WAN ポートをシンプルな“アクティブ/パッシブ”セットアップで使用して、プライマリ WAN ポートが利用不可能になったときに限り、トラフィックをバックアップ WAN ポートを介して転送することができます。この方法で、セカンダリ WAN ポートに“フェイルオーバー”することによって、SonicWall は WAN ポートトラフィック用に恒久的な接続を維持できます。

WWAN インターフェースを備えた SonicWall 装置の場合は、WWAN インターフェースを使用してフェイルオーバーを設定することができます。イーサネット WAN（WAN ポート、OPT ポート、またはその両方）と WWAN 間のフェイルオーバーは、**WAN 接続モデル**の設定を介してサポートされます。

この機能によって、SonicWall 上の WAN トラフィックに対してシンプルな負荷分散（LB）を行うこともできます。2 つの WAN ポート間の発信 WAN トラフィックを分割する方法を選択して、ネットワークトラフィックを分散させることができます。現在、負荷分散はイーサネット WAN インターフェースでのみサポートされています。

SonicOS は、リンクの電源オフまたは切断を検出する物理監視、またはアップストリーム接続の中断など、より高いレベルでトラフィックを監視する物理および論理監視を使用して WAN トラフィックを監視できます。

ⓘ **重要:** 開始する前に、WAN ポート設定をミラーリングするようにユーザ定義のインターフェースが設定されていることを確認してください。

トピック:

- 設定
- グループ

設定

SonicWall 装置の WAN フェイルオーバーを設定するには、次の手順に従います。

1. 「**ネットワーク | システム > フェイルオーバー & 負荷分散**」ページに移動します。

2. 「**負荷分散を有効にする**」を選択します。LB グループと LB 統計のセクションにアクセスするためには、このオプションを有効にする必要があります。これが無効になっていると、フェイルオーバーと負荷分散に関するオプションを設定することはできません。このオプションは、既定では選択されています。
3. 「**プローブに応答する**」を選択します。これを有効にすると、装置が自らのインターフェースのいずれかに着信したプローブ要求パケットに応答できます。このオプションは、既定では選択されていません。このオプションを有効にすると、「**次のポートへのすべての TCP-SYN**」オプションが使用可能になります。
4. 「**次のポートへのすべての TCP-SYN**」を選択します。
   - 「**プローブに応答する**」オプションが有効になっている場合のみ、このオプションを使用できます。このオプションを選択すると、装置は設定値と同じ送信先アドレス TCP ポート番号を持つ TCP プローブ要求パケットにのみ応答します。既定の TCP ポート番号は **0** です。
   - このオプションは、既定では選択されていません。
5. 「**適用**」を選択します。

グループ

グループの設定を行うには、以下の手順に従います。

1. 「**ネットワーク | システム > フェイルオーバー & 負荷分散**」ページに移動します。
2. 「**ネットワーク | システム > フェイルオーバー & 負荷分散**」ページの「**グループ**」テーブルで、設定したいグループの**設定**アイコンを選択します。「**LB グループの修正**」ダイアログが表示されます。

3. 「**発信の負荷分散方法**」セクションから、負荷分散の種別（方法）を選択します。オプションは選択した種別に応じて変化します。

   - **基本のアクティブ/パッシブ フェイルオーバー** — 「**可能な際にはプライマリ インターフェースが先制してフェイルバックする**」が有効な場合、4 つの WAN インターフェースが順位を使用して優先順序を決定します。アクティブな WAN インターフェースに優先することができるのは、より高い順位のインターフェースのみです。これは、既定で選択されています。
   - **接続毎のラウンド ロビン** — ラウンド ロビン方式で選択する WAN インターフェースの順序を変更できるようになりました。既定の順序は次のとおりです。

     - プライマリ WAN 割合
     - バックアップ #1 割合
     - バックアップ #2 割合
     - バックアップ #3 割合

     その後、プライマリ WAN に戻ってこの順序が繰り返されます。
   - **スピルオーバー** — 帯域幅のしきい値がプライマリ WAN に適用されます。しきい値を超えると、新しいトラフィック フローはラウンド ロビン方式でバックアップ WAN に割り当てられます。プライマリ WAN の帯域幅が設定済みしきい値を下回ると、ラウンド ロビンは停止し、新しい送信フローは再びプライマリ WAN のみを介して送信されるようになります。

     ⓘ **補足:** 現存するフローは（既にキャッシュされているので）正常にタイムアウトするまではバックアップ WAN に関連付けられたままになります。
   - **使用比率** — LB グループの WAN ごとに比率を設定できます。設定エラー関連の問題を回避するために、比率と WAN インターフェースが正しく対応していることを確認してください。
4. 「**発信の負荷分散方法**」から選択した内容に応じて、以下のオプションのいずれかが表示されます。

種別ドロップダウンのオプション

選択した種別	オプション
基本のアクティブ/パッシブ フェイルオーバー	**可能な際にはプライマリ インターフェースが先制してフェイルバックする** このオプションを選択すると、先制の順序を決める階級すなわち順位が有効になります。既定で選択されています。
スピルオーバー	**帯域幅がプライマリ インターフェースの帯域幅制限 (Kbits/秒) を超えると、新しいフローはラウンド ロビン方式でバックアップ グループ メンバーに向けられる。** このフィールドでプライマリ インターフェースの帯域幅を指定します。この値を超えた場合、新しいフローは「選択済み」列の表示順序に従ってバックアップ グループ メンバーに送信されます。このオプションは、既定では選択されていません。既定値は 0 です。
ラウンド ロビン、スピルオーバー、割合	**送信元と送信先 IP アドレス バインディングを使う** このオプションは、HTTP/HTTPS リダイレクトを使用している場合などに特に便利です。例えば、接続 A と接続 B が同じ WAN インターフェース上に存在する必要があり、接続 A での送信元および送信先 IP アドレスが接続 B のものと同じであるが、異なるサービスが使用されている場合などです。この場合、トランザクションがエラーにならないように同じ WAN インターフェース上で両方の接続を維持するために、送信元および送信先の IP アドレスのバインドが必要です。このオプションは、既定では選択されていません。

5. メンバー インターフェースの追加、削除、並べ替えを「**グループ メンバー**」、ここを選択:/選択済 **プライマリ/バックアップ プール:**」リストで行います。「**選択済み**」リストの選択済みメンバーの用途は、選択した**種別**によって異なります。
   - **基本のアクティブ/パッシブ フェイルオーバー: インターフェース順序:**
   - **接続毎のラウンド ロビン: インターフェース プール:**
   - **スピルオーバー: プライマリ/バックアップ プール:**
   - **割合: インターフェース分配:**
6. メンバーを追加するには、「**グループ メンバー:**」列に表示されるインターフェースを選択し、「**追加>>**」を選択します。

   「**割合**」を選択した場合は、エントリを並べ替える代わりに、各インターフェースの帯域幅の割合を指定できます。「*割合による帯域幅の設定*」を参照してください。

   ⓘ **重要:** 設定エラー関連の問題を回避するために、比率と WAN インターフェースが正しく対応していることを確認してください。

   a. インターフェースに割り当てる帯域幅の比率を「パーセント (%)」フィールドに入力します。すべてのインターフェースの帯域幅の合計が 100% となるようにしてください。割り当てた帯域幅の合計パーセントが表示されます。

   「**選択済:**」列のメンバーを削除するには、次の操作を行います。

   1. 表示されたインターフェースを選択する。
   2. 「**<<削除**」を選択します。

   ⓘ **補足:** リストの先頭に表示されるインターフェースがプライマリです。
   個々のメンバーに対して実行される処理はインターフェースの順位では決まりません。実行される処理は、グループ種別で指定されます。
7. 「**OK**」を選択します。

8. 「**プローブ**」タブに入力します。

3

近隣者検出

近隣者検出プロトコル（NDP）は、IPv4 の ICMP と ARP が実現できるいくつかのタスクを実行するために IPv6 の一部として作成された、メッセージング プロトコルです。ARP と同じように、近隣者検出によって動的エントリ（登録）のキャッシュが構築されます。静的な近隣者検出のエントリ（登録）は設定することができます。IPv4/IPv6 近隣者の表に、従来の IPv4 近隣者メッセージと類似した IPv6 近隣者メッセージと機能を示します。

IPV4/IPV6 近隣者メッセージと機能

IPv4 近隣者メッセージ	IPv6 近隣者メッセージ
ARP 要求メッセージ	近隣者要請メッセージ
ARP 応答メッセージ	近隣者広告メッセージ
ARP キャッシュ	近隣者キャッシュ
重複回避用 ARP	重複アドレス検出
ルータ要請メッセージ（オプション）	ルータ要請（必須）
ルータ広告メッセージ（オプション）	ルータ広告（必須）
リダイレクト メッセージ	リダイレクト メッセージ

静的 NDP 機能により、レイヤ 3 IPv6 アドレスとレイヤ 2 MAC アドレスとの間に静的割付を作成できます。

トピック:

- 静的 NDP 登録
- NDP 設定
- NDP キャッシュ

静的 NDP 登録

IP アドレス	リモート機器の IPv6 IP アドレス。
MAC アドレス	リモート機器の MAC アドレス。
ベンダー	リモート機器の製造元の名前。
インターフェース	リモート機器に関連付けられているインターフェース。
構成	マウス ポインタを置くと、この登録の**編集**アイコンと**削除**アイコンが表示されます。

静的 NDP 登録の追加

静的 NDP 登録を追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > 近隣者検出**」ページに移動します。

2. 「**静的 NDP 登録**」テーブルで、「**+ 追加**」を選択します。「**静的 NDP の追加**」ダイアログが表示されます。

3. 「**IP アドレス**」フィールドに、リモート機器の IPv6 アドレスを入力します。
4. 「**インターフェース**」から、この登録で使用する SonicWall 装置上のインターフェースを選択します。
5. 「**MAC アドレス**」フィールドに、リモート機器の MAC アドレスを入力します。
6. 「**追加**」を選択します。静的 NDP 登録が追加されます。

静的 NDP 登録の編集

静的 NDP 登録を編集するには、以下の手順に従います。

1. 「**静的 NDP 登録**」テーブルで、マウス ポインタを置いた登録の「**この登録を編集する**」アイコンを選択します。「**静的 NDP の編集**」ダイアログが表示されます。

2. 変更を加えます。
3. 「**更新**」を選択します。エントリが更新されます。

静的 NDP 登録の削除

静的 NDP 登録の削除が必要な場合があります。

「静的 NDP 登録」テーブルの登録を削除するには、以下の手順に従います。

1. 登録にマウス ポインタを置き、「**削除**」アイコンまたは「**この登録を削除する**」アイコンを選択します。

「静的 NDP 登録」テーブルの 1 つ以上の登録を削除するには、以下の手順に従います。

1. 削除する 1 つ以上の登録のチェックボックスをオンにします。
2. 「**削除**」を選択します。

「静的 NDP 登録 キャッシュ」テーブル内のすべての登録を消去するには、以下の手順に従います。

1. 「**静的 NDP 登録**」テーブルの見出しの左上にあるチェックボックスをオンにします。
2. 「**削除**」を選択します。

NDP 設定

「NDP 設定」で、近隣者に到達するための最大時間を指定します。

ⓘ **補足:** IPv6 では、「**ネットワーク | システム > インターフェース | インターフェースの編集 > 詳細**」ダイアログで、この値を各インターフェースに対して設定することもできます。インターフェースで**ルータ通知**が有効になっている場合、あるインターフェースに対して設定されている値はそのインターフェースでのみ使用されます。詳細については、「*インターフェースの設定*」を参照してください。

最大時間を指定するには、以下の手順に従います。

1. 「**ネットワーク | システム > 近隣者検出 | NDP 設定**」ビューに移動します。

2. 「**近隣者検出の基準到達可能時間 (秒)**」フィールドに数値を入力します。最小値は **0** 秒、最大値は **3600** 秒、既定値は **20** 秒です。

ⓘ | **ヒント:** このオプションの値が **0** に設定されている場合は、NDP 設定のグローバル値が使用されます。

3. **変更** をクリックします。

NDP キャッシュ

NDP キャッシュ テーブルに、現在のすべての IPv6 近隣者が表示されます。

IP アドレス	近隣者機器の IPv6 IP アドレス。
種別	近隣者の種別: • **REACHABLE** — 近隣者は 30 秒以内で到達可能であると認識されています。 • **STALE** — 近隣者はすでに到達可能であると認識されていなく、その近隣者に 1200 秒以内にトラフィックが送信されています。 • **STATIC** — 近隣者は静的近隣者として手動で設定されました。
MAC アドレス	近隣者機器の IPv6 MAC アドレス。
ベンダー	近隣者機器の製造元の名前。
インターフェース	この近隣者機器に関連付けられているインターフェース。
タイムアウト	ユーザがタイムアウトするまでの無動作時間の長さ。
消去	エントリの**削除**アイコンがあります。

NDP キャッシュの消去

ネットワーク上の機器の IP アドレスが変更された場合は、NDP キャッシュの消去が必要になることがあります。IP アドレスは物理アドレスにリンクされるので、変更された IP アドレスは「NDP キャッシュ」内で物理アドレスに関連付けられたままです。「NDP キャッシュ」を消去すると、新しい情報が収集され、NDP キャッシュに保管されます。

ⓘ | **ヒント:** 登録がタイムアウトするまでの時間を設定するには、「「NDP キャッシュ」登録タイムアウト (分)」フィールドに時間を分単位で入力します。次を参照してください。「NDP 設定」.

「NDP キャッシュ」テーブルの登録を消去するには、以下の手順に従います。

1. NDP キャッシュ登録にマウス ポインタを置き、右側にある「**消去**」アイコンを選択します。

「NDP キャッシュ」テーブル内の 1 つ以上の登録を消去するには、以下の手順に従います。

1. 消去する 1 つ以上のエントリのチェックボックスをオンにします。
2. NDP キャッシュ登録にマウス ポインタを置き、「**消去**」を選択します。

「NDP キャッシュ」テーブル内のすべての登録を消去するには、以下の手順に従います。

1. 「**NDP キャッシュ**」テーブルのヘッダーの左上にあるチェックボックスをオンにします。すべての NDP キャッシュ登録が選択されます。
2. 登録にマウス ポインタを置き、「**消去**」または「**すべて消去**」を選択します。

4

ARP

ARP (Address Resolution Protocol) は、第 3 層 (IP アドレス) を第 2 層 (物理アドレスまたは MAC アドレス) に割り付け、同じサブネットに存在するホスト間の通信を可能にします。ARP は、ネットワークのトラフィックを増大させるブロードキャスト プロトコルです。ブロードキャスト トラフィックを最小限にするために、ARP キャッシュが保持されており以前に取得された ARP 情報が保管および再使用されます。

トピック:

- 静的 ARP 登録
- ARP 設定
- ARP キャッシュ

静的 ARP 登録

静的 ARP 登録機能により、レイヤ 2 MAC アドレスとレイヤ 3 IP アドレスとの間に静的マッピングを作成できます。

トピック:

- 静的 ARP エントリの表示
- 静的 ARP 登録の追加
- 静的 ARP 登録の編集
- 静的 ARP 登録の削除
- 静的 ARP によるセカンダリ サブネット

静的 ARP エントリの表示

IP アドレス	ゲートウェイの役割を果たすセキュリティ装置の IP アドレス。
MAC アドレス	ゲートウェイの役割を果たすセキュリティ装置の MAC アドレス。
ベンダー	セキュリティ装置のメーカーの名前。
インターフェース	このエントリに関連付けられている LAN インターフェース。

公開	緑色のチェックマークにより、セキュリティ装置が指定された IP アドレスに対する ARP クエリに指定された MAC アドレスで応答するかどうかを示します。
バインド MAC	緑色のチェックマークにより、指定された IP アドレスおよびインターフェースに MAC アドレスがバインドされているかどうかを示します。

静的 ARP 登録の追加

静的 ARP 登録を追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > ARP**」に移動します。
2. 「**静的 ARP 登録**」ビューで、プラス記号 (**+**、**静的 ARP の追加**) を選択します。「**静的登録の追加**」ダイアログが表示されます。

3. 「**IP アドレス**」フィールドに、SonicWall 装置の IP アドレスを入力します。
4. 「**インターフェース**」で、この静的 ARP 登録と関連付けられる装置上のインターフェースを選択します。
5. 「**MAC アドレス**」フィールドに、装置の MAC アドレスを入力します。
6. 装置が、指定された IP アドレスに対する ARP クエリに、指定された MAC アドレスで応答するようにするには、「**この登録を公開する**」オプションを選択します。このオプションは、既定では選択されていません。

   このオプションを使用すると、例えば、セキュリティ装置の MAC アドレスを追加して、その装置で特定のインターフェースのバックアップの IP アドレスに応答できるようになります。このオプションを選択すると、「**MAC アドレス**」フィールドと「**MAC アドレスをバインドする**」オプションが淡色表示になります。
7. 「**この登録を公開する**」を選択した場合は、**「保存」を選択します。**。
8. 指定された MAC アドレスを目的の IP アドレスおよびインターフェースにバインドするには、「**MAC アドレスを割り当てる**」を選択します。このオプションは、既定では選択されていません。

   このオプションにより、(ネットワーク カードの一意の MAC アドレスで認識される) 特定のワークステーションを、装置上の指定のインターフェースでのみ使用できるようになります。MAC アドレスが 1 つのインターフェースにバインドされた後、装置は次のように動作します。

   - 他のどのインターフェースでもその MAC アドレスに応答しなくなります。
   - 存在している可能性がある、その MAC アドレスに対する動的にキャッシュされた参照をすべて削除します。
   - その MAC アドレスへの追加的な (一意でない) 静的割付を禁止します。

     「**MAC アドレスを割り当てる**」を選択すると、「**IP アドレスを動的に更新する**」が使用可能になります。
9. DHCP を動的な IP アドレスの割り当てに使用するときに MAC アドレスをインターフェースにバインドできるようにするには、「**IP アドレスを動的に更新する**」を選択します、これは「**MAC アドレスをバインドする**」オプ

ションのサブ機能です。

このオプションを有効にすると、「**IP アドレス**」フィールドが淡色表示になって 0.0.0.0 に設定され、「**MAC アドレス**」フィールドが使用可能になり、装置の内部 DHCP サーバによって割り当てられた IP アドレス（IP ヘルパーを使用中の場合は外部 DHCP サーバによって割り当てられた IP アドレス）が **ARP キャッシュ**に格納されます。

10. 「**保存**」を選択します。

静的 ARP 登録の編集

静的 ARP 登録を編集するには、以下の手順に従います。

1. 「**ネットワーク | システム > ARP**」に移動します。
2. 「**静的 ARP 登録**」ビューで、登録の右側にある**編集**アイコンにマウス ポインタを置きます。「**静的登録の追加**」ダイアログが表示されます。

3. 必要な変更を行います。
4. 「**保存**」を選択します。エントリが更新されます。

静的 ARP 登録の削除

「静的 ARP 登録」テーブルから静的 ARP 登録を削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > ARP | 静的 ARP 登録**」ビューに移動します。
2. 削除する登録の横にあるチェックボックスをオンにします。
3. 登録の右側にある**ゴミ箱**アイコンにマウス ポインタを置いて、選択します。
4. 確認のダイアログ ボックスが表示されたら、「**確認**」を選択します。

「静的 ARP 登録」テーブルからすべての静的 ARP 登録を削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > ARP | 静的 ARP 登録**」ビューに移動します。
2. テーブルのタイトル行の左上にあるチェックボックスをオンにします。すべての**静的 ARP 登録**が選択されます。
3. テーブルの右側にある**ゴミ箱**アイコンを選択します。
4. 確認のダイアログ ボックスが表示されたら、「**確認**」を選択します。

静的 ARP によるセカンダリ サブネット

静的 ARP 機能により、自動 NAT ルールを追加せずにセカンダリ サブネットを別のインターフェースに追加できます。

トピック:

- セカンダリ サブネットの追加
  - セカンダリ サブネットの例

セカンダリ サブネットの追加

静的 ARP 方式を使用してセカンダリ サブネットを追加するには、以下の手順に従います。

1. セカンダリのサブネットに使用するゲートウェイ アドレスの静的 ARP エントリを、「*公開*」オプションを有効に設定して追加し、その ARP に、接続する装置インターフェースの MAC アドレスを割り当てます。
2. セカンダリのサブネットへの静的ルートを追加します。これにより、装置がそれを有効なトラフィックと見なすようになり、そのサブネットのトラフィックをどのインターフェースにルーティングすべきかが認識されます。
3. アクセス ルールを追加して、サブネットへのトラフィックが正しいネットワーク インターフェースを通過できるようにします。
4. *必要に応じて*、アップストリームの機器に静的ルートを追加し、どのゲートウェイ IP を使用すればセカンダリのサブネットに到達可能かを識別できるようにします。

セカンダリ サブネットの例

次のネットワークの例について考えます（次を参照してください）。「セカンダリ サブネットの追加」.

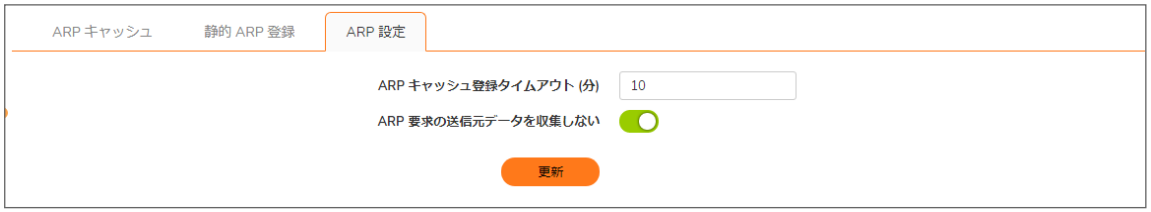
追加された構成をサポートするには、以下の手順に従います。

1. セカンダリ サブネットのゲートウェイとなるアドレス、`10.203.28.57` について、公開される静的 ARP エントリを作成します。これを適切な LAN インターフェースと関連付けます。
2. 「**ネットワーク | システム > ARP | 静的 ARP 登録**」ビューに移動します。
3. **静的 ARP の追加** (+) アイコンを選択します。
4. 次のエントリを追加します。

5. 「**保存**」を選択します。エントリは「**静的 ARP**」テーブルに表示されます。
6. 「**ネットワーク | システム > 動的ルーティング**」に移動します。
7. サブネット マスク `255.255.255.0` を指定して、ネットワーク `10.203.28.57` への静的ルートを X3 インターフェース上に追加します。静的ルートの追加の詳細については、「*ルート通知とルート ポリシーの設定*」を参照してください。

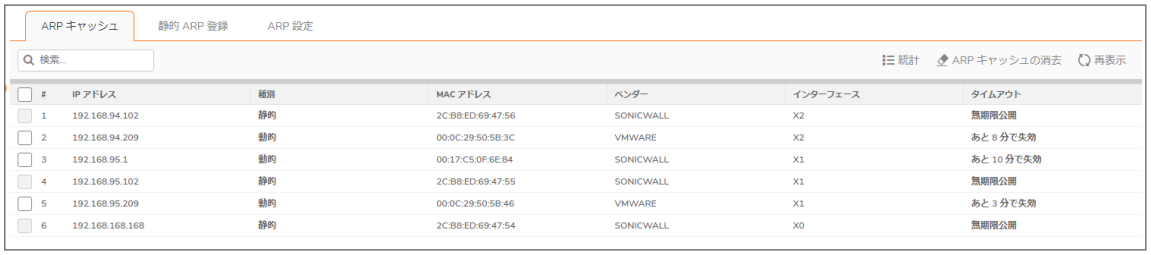
8. トラフィックがサブネット 10.203.28.57 に到達し、またそのサブネットが LAN 上のホストに到達できるようにするために、「**ポリシー | ルールとポリシー > アクセス ルール**」ページに移動します。
9. トラフィックの通過を許可するための適切なアクセス ルールを追加します。

ARP 設定



ARP キャッシュ登録タイムアウト (分)	登録がタイムアウトしてキャッシュから消去されるまでの時間を指定します。最小値は 2 分、最大値は 600 分 (10 時間)、既定値は **10** 分です。
ARP 要求の送信元データを収集しない	ARP 要求から送信元データが取得されないようにします。このオプションは、既定では選択されていません。

ARP キャッシュ



IP アドレス	装置の IP アドレス。
種別	ARP が**静的**または**動的**のどちらであるかを示します。
MAC アドレス	IP アドレスと関連付けられている MAC アドレス。
ベンダー	セキュリティ装置のメーカーの名前。
インターフェース	この ARP 登録に関連付けられている LAN インターフェース。
タイムアウト	このエントリについてキャッシュの残り時間を示します。設定時にエントリが公開されていた場合、「**タイムアウト**」には「**無期限公開**」と表示されます。
消去	**ARP キャッシュ**からエントリを消去するための**削除**アイコンを表示します。 ⓘ | **補足: 削除**アイコンは**動的**エントリでのみ使用できます。

トピック:

- ARP キャッシュの消去

ARP キャッシュの消去

ネットワーク上の機器の IP アドレスが変更された場合は、ARP キャッシュを消去する必要があります。IP アドレスは物理アドレスにリンクされるので、変更された IP アドレスは ARP キャッシュ内で物理アドレスに関連付けられたままです。ARP キャッシュを消去すると、新しい情報が収集され、ARPキャッシュに保管されます。

ヒント: 登録がタイムアウトするまでの時間を設定するには、「**ARP キャッシュ登録タイムアウト（分）**」フィールドに時間を分単位で入力します。次を参照してください。「ARP 設定」.

「ARP キャッシュ」テーブル内の 1 つの動的登録を消去するには、以下の手順に従います。

1. 登録の右側にマウス ポインタを置いて、「**ARP キャッシュの消去**」アイコンを選択します。

「ARP キャッシュ」テーブル内の 1 つ以上の動的登録を消去するには、以下の手順に従います。

1. 消去する 1 つ以上の登録のチェックボックスをオンにします。「消去」が使用可能になります。
2. 「**ARP キャッシュの消去**」アイコンを選択します。

「ARP キャッシュ」テーブル内のすべての動的登録を消去するには、以下の手順に従います。

1. 見出し行の左上にあるチェックボックスをオンにします。すべての動的登録が選択されます。
2. 「**ARP キャッシュの消去**」アイコンを選択します。

5

MAC IP アンチスプーフ

MAC および IP アドレスをベースにした攻撃は、今日のネットワーク セキュリティ環境でますます一般化しています。この種の攻撃は、ローカル エリア ネットワーク（LAN）を標的にすることが多く、ネットワークの外部からも内部からも行われることがあります。実際、オフィスの会議室、学校、図書館など、内部 LAN がある程度公開されている場所ならどこでも、この種の攻撃の緒になる可能性があります。これらの攻撃にはさまざまな異名があり、man-in-the-middle 攻撃、ARP ポイズニング、SPITS などと呼ばれています。MAC-IP アンチスプーフ機能は、ネットワークへのアクセスを制御する種々の方法を管理者に提供し、OSI レイヤ 2/3 へのスプーフィング攻撃を排除することにより、これらの攻撃のリスクを減じます。

MAC-IP アンチスプーフ機能は 2 つの点に重点的に取り組んでいます。その 1 つは受付制御です。これにより、どの機器にネットワークへのアクセスを許すかを選択できます。もう 1つは、第 2 層へのサービス拒否攻撃などのスプーフィング攻撃の排除です。これらの目標を達成するためには、2 つの情報キャッシュを構築する必要があります。それは MAC-IP アンチスプーフ キャッシュと ARP キャッシュです。

MAC-IP アンチスプーフ キャッシュは、受信パケットを検証し、ネットワーク内に入れてよいかどうかを判定するためのものです。受信パケットの送信元の MAC アドレスと IP アドレスがこのキャッシュ内から検索されます。それらのアドレスが見つかれば、そのパケットの通過が許可されます。MAC-IP アンチスプーフ キャッシュは、次のサブシステムのうちの 1 つ以上のものから構築されます。

- DHCP サーバベースのリース（SonicWall — DHCP サーバ）
- DHCP リレーベースのリース（SonicWall — IP ヘルパー）
- 静的 ARP エントリ
- ユーザ作成の静的エントリ

ARP キャッシュは次のサブシステムから構築されます。

- ARP パケット（ARP 要求と ARP 応答の両方）
- ユーザ作成エントリからの静的 ARP エントリ
- MAC-IP アンチスプーフ キャッシュ

MAC-IP アンチスプーフ サブシステムは、ARP キャッシュをロックすることで送信（イーグレス）制御を実現し、不正な機器や望ましくない ARP パケットによって送信パケット（ネットワークから出ていくパケット）がなりすましに利用されないようにします。これにより、マッピングに基づいてファイアウォールで意図しない機器にパケットがルーティングされるのを防ぎます。また、ARP キャッシュ内のクライアントの MAC アドレスを更新して、man-in-the-middle 攻撃も防ぎます。

トピック:

- MAC IPv4 および IPv6 アンチスプーフ設定
- MAC-IP アンチスプーフの設定
- アンチスプーフ キャッシュ
- スプーフ検知リスト

MAC IPv4 および IPv6 アンチスプーフ設 定

MAC IPv4 アンチスプーフ設定を編集するには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」ページに移動します。
2. 「**IPv4**」ビューを選択します。

MAC IPv6 アンチスプーフ設定を編集するには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」ページに移動します。
2. 「**IPv6**」ビューを選択します。

MAC-IP アンチスプーフの設 定

特定のインターフェースについて設定を行うには、そのインターフェースの「**設定**」列の**編集**アイコンを選択します。選択されたインターフェースに対する「**インターフェースの編集**」ダイアログが表示されます。

使用できるオプションは次のとおりです。

- **アンチスプーフ設定**
  - **有効 – MAC–IP ベースのアンチスプーフを有効にする**: このインターフェースによるトラフィックに関して MAC–IP アンチスプーフ サブシステムを有効にします。
  - **静的 ARP**: 静的 ARP 登録からアンチスプーフ キャッシュを構築できるようにします。
  - **DHCP サーバ**: SonicWall DHCP サーバからのアクティブな DHCP リースからアンチスプーフ キャッシュを構築できるようにします。
  - **DHCP リレー**: IP ヘルパーに基づいて DHCP リレーからのアクティブな DHCP リースからアンチスプーフ キャッシュを構築できるようにします。
- **ARP 設定**
  - **ARP ロック**: MAC–IP アンチスプーフ キャッシュ内にリストされている機器について ARP 登録をロックします。これは MAC–IP アンチスプーフ設定を通じてインターフェースの送信制御に適用され、MAC–IP キャッシュ エントリが ARP キャッシュ内の永続的なエントリとして追加されます。これにより、ARP ポイズニング攻撃が規制されます。不正な ARP パケットによって ARP キャッシュが変更されないからです。

- **ARP 監視**: 接続されているマシンの ARP 汚染を防ぎ、すべてのクライアント PC を man-in-the-middle 攻撃から保護します。

- **その他の設定**
  - **受信アンチスプーフの強制**: インターフェースでの受信（イングレス）制御を可能にして、MAC-IP アンチスプーフ キャッシュにリストされていない機器からのトラフィックをブロックします。
  - **スプーフ検知**: アンチスプーフ キャッシュをパスできなかった機器をすべて記録し、それらの機器を「**スプーフ検知リスト**」に記載します。
  - **管理の許可**: **アンチスプーフ キャッシュ**に現在リストされていない機器からのものも含めて、装置の IP アドレスに宛てられたすべてのパケットの通過を許可します。

このインターフェースの選択内容の設定終了後、「**保存**」を選択します。設定の調整が行われた後、「MAC-IP アンチスプーフ」ページでインターフェースのリストが更新されます。緑の円に白のチェック マークが入ったアイコンによって、どの設定が有効になっているのかがわかります。

ⓘ | **補足:** MAC-IP アンチスプーフ リストから除外されているインターフェースは、

- 非イーサネット インターフェース
- Portshield メンバー インターフェース
- レイヤ 2 ブリッジ ペア インターフェース
- 高可用性インターフェース
- 高可用性データ インターフェース

アンチスプーフ キャッシュ

MAC-IP アンチスプーフ キャッシュには、ネットワークへのアクセスが許可されているすべての機器と、ネットワークから排除された（アクセスを拒否された）すべての機器がリストされます。

リストに機器を追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」ページに移動します。
2. 「**+ 追加**」を選択します。「**アンチスプーフ キャッシュの追加**」ダイアログが表示されます。

3. 「**インターフェース**」からインターフェースを選択します。
4. 「**IP アドレス**」フィールドに機器の IP アドレスを入力します。

5. 「**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。
6. 「ルータ」オプションを選択すると、その機器の背後から来るトラフィックが許可されます。
7. 「**ブラックリストに登録されたデバイス**」オプションを選択すると、その IP アドレスに関係なく、その機器からのパケットが遮断されます。
8. 「**保存**」を選択します。

アンチスプーフ キャッシュ登録を編集する必要がある場合は、その登録の「**設定**」列にある**編集**アイコンを選択します。

1 つまたは複数のアンチスプーフ キャッシュ登録を削除できます。それには、各登録の横のチェックボックスをオンにし、「**MAC-IP アンチスプーフ キャッシュの削除**」を選択します。

キャッシュ統計を消去するには、以下の手順に従います。

1. 目的の機器を選択し、「**リセット**」を選択します。

MAC-IP アンチスプーフ機能を有効にしていても、次のタイプのパケットはこの機能をバイパスします。

- 非 IP パケット。
- 送信元 IP が 0 である DHCP パケット。
- VPN トンネルからのパケット。
- 送信元 IP が無効なユニキャスト IP であるパケット。
- アンチスプーフの設定で管理の状態が有効になっていないインターフェースからのパケット。

「アンチスプーフ キャッシュの検索」セクションでは、キャッシュ内の登録を検索することができます。

MAC-IP アンチスプーフ キャッシュを検索するには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」ページに移動します。
2. フィールドに検索文字列を入力します。
3. 「**検索**」を選択します。MAC-IP アンチスプーフ キャッシュ内の一致する登録が表示されます。

「アンチスプーフ キャッシュ」テーブルを消去して、すべての登録を再表示するには、「**再表示**」を選択します。

スプーフ検 知リスト

ⓘ | **補足:** 「スプーフ検知リスト」表示は、装置レベルでのみ使用可能です。

スプーフ検知リストには、受信アンチスプーフ キャッシュ チェックをパスできなかった機器が表示されます。このリストのエントリは、静的アンチスプーフ エントリとして追加できます。

「スプーフ検知リスト」を表示するには、以下の手順に従います。

1. 「**Request Spoof Detected List from Firewall (ファイアウォールからスプーフ検知リストを要求する)**」を選択します。

「**消去**」を選択すると、リストから登録を消去することができます。「**解決**」を選択すると、NetBIOS を使用して各機器の名前を解決することができます。

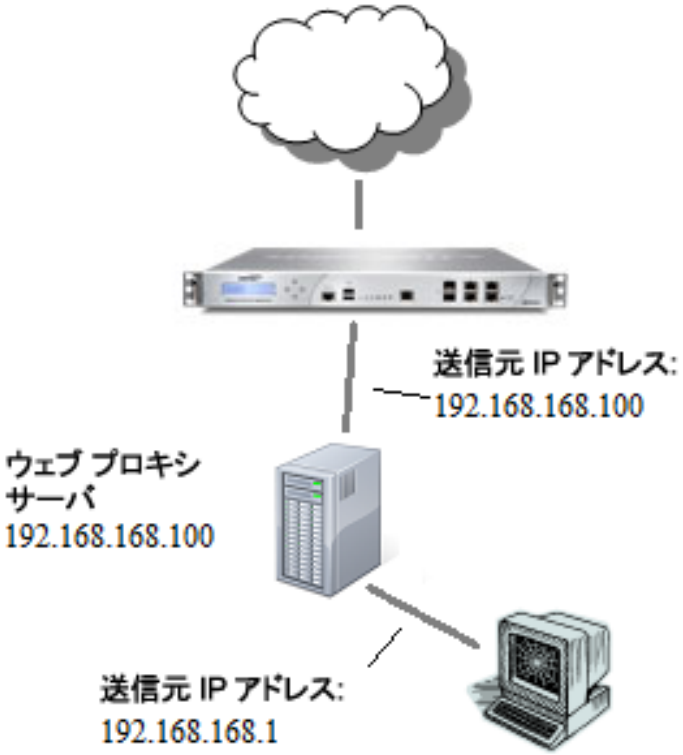
静的アンチスプーフ リストに登録を追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」ページに移動します。
2. 目的の機器の「**追加**」列にある**編集**アイコンを選択します。警告メッセージ ウィンドウが開き、この静的エントリを追加するかどうか尋ねられます。
3. 「**OK**」を選択して続行します。

6

ウェブ プロキシ

内部ネットワーク（ユーザと SonicWall 装置の間）にあるプロキシ サーバを通じてユーザがウェブにアクセスすると、装置からはユーザではなくプロキシ サーバから HTTP/HTTPS 接続が行われているように認識されます。



トピック:

- 自動プロキシ転送（ウェブのみ）
- ユーザ プロキシ サーバ
  - ユーザ プロキシ サーバの追加
  - ユーザ プロキシ サーバの編集
  - ユーザ プロキシ サーバの削除

ユーザ プロキシ サーバ

ウェブ プロキシ サーバは HTTP 要求をインターセプトし、要求されたウェブ ページのコピーを保管しているかどうかを判別します。保管していない場合、プロキシはインターネット上のサーバへの要求を完了し、要求された情報を返すとともに将来の要求に備えてローカルに保存します。ネットワーク上の各コンピュータがウェブ要求をサーバに送る設定をする必要があるため、ネットワーク上のウェブ プロキシ サーバのセットアップは手間がかかる場合があります。

プロキシ サーバがネットワーク上にある場合は、各コンピュータのウェブ ブラウザがプロキシ サーバに接続するように設定する代わりに、サーバを WAN または DMZ ゾーンに移動し、「**ネットワーク | システム > ウェブ プロキシ**」ページの設定を使用して、ウェブ プロキシ転送を有効にすることができます。装置によってすべてのウェブ プロキシ要求が自動的にプロキシ サーバに転送され、ネットワーク上のすべてのコンピュータを設定する必要はありません。

自 動 プロキシ転 送 (ウェブのみ)

ウェブ プロキシ サーバは HTTP 要求をインターセプトし、要求されたウェブ ページのコピーを保管しているかどうかを判別します。保管していない場合、プロキシはインターネット上のサーバへの要求を完了し、要求された情報をユーザに返すとともに将来の要求に備えてローカルに保存します。

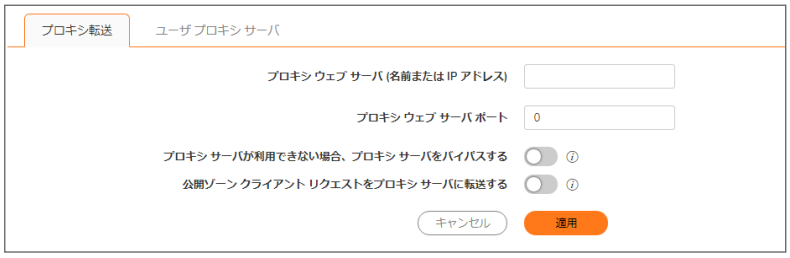
ネットワーク上の各コンピュータがウェブ要求をサーバに送る設定をする必要があるため、ネットワーク上のウェブ プロキシ サーバのセットアップは手間がかかる場合があります。

プロキシ サーバが SonicWall 装置のネットワーク上にある場合は、装置をネットワークとプロキシ サーバの間に移動して、「**ウェブ プロキシ転送**」を有効にすることができます。これによってすべての WAN 要求がプロキシ サーバに転送され、コンピュータを個別に設定する必要はありません。

ⓘ | **補足:** プロキシ サーバは WAN または DMZ に配置しなければなりません。LAN に配置することはできません。

プロキシ ウェブ 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 | システム > ウェブ プロキシ**」ページに移動します。



2. 「**プロキシ ウェブ サーバ (名前または IP アドレス)**」フィールドに、プロキシ サーバの名前または IP アドレスを入力します。
3. 「**プロキシ ウェブ サーバのポート番号**」フィールドに、プロキシの IP ポートを入力します。
4. 障害が発生した場合にプロキシ サーバをバイパスするには、「**プロキシ サーバが利用できない場合、プロキシ サーバをバイパスする**」を有効にします。このオプションにより、ウェブ プロキシ サーバが利用できなくなったときに、装置の背後にあるクライアントがウェブ プロキシ サーバをバイパスできるようになります。代

わりに、クライアントのブラウザは、ウェブ プロキシ サーバが指定されていないかのようにインターネットに直接アクセスします。

5. 公開ゾーンにあるクライアントにもプロキシ サーバを強制的に使わせるには、「**公開ゾーン クライアント リクエストをプロキシ サーバに転送する**」を有効にします。
6. 「**適用**」を選択します。

装置が更新された後、更新を確認するメッセージが表示されます。

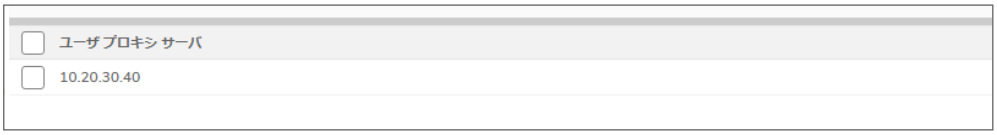
説明とスケジュールを確認してください。

ユーザ プロキシ サーバの追加

ユーザのウェブ リクエストを経由させるウェブ プロキシ サーバを追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > ウェブ プロキシ**」ページに移動します。
2. 「**ユーザ プロキシ サーバ**」セクションで、「**+ ユーザ プロキシ サーバの追加**」を選択します。「**プロキシ サーバの追加**」ダイアログが表示されます。

3. 「**プロキシ サーバのホスト名または IP アドレスの入力**」フィールドに、プロキシ サーバのホスト名または IP アドレスを入力します。
4. 「**適用**」を選択します。「**ユーザ プロキシ サーバ**」テーブルに新しいプロキシ サーバが表示されます。



5. 「**適用**」を選択します。

ユーザ プロキシ サーバの編集

ウェブ プロキシ サーバを編集するには、以下の手順に従います。

1. 「**ネットワーク | システム > ウェブ プロキシ**」ページに移動します。
2. 「**ユーザ プロキシ サーバ**」テーブルで、変更するプロキシ サーバを選択し、「**この登録を編集する**」アイコンの上にマウス ポインタを置きます。
3. 「**この登録を編集する**」を選択します。「**プロキシ サーバの編集**」ダイアログが表示されます。

4. 「**プロキシ サーバのホスト名または IP アドレスの入力**」フィールドに変更を加えます。
5. 「適用」を選択します。「**ユーザ プロキシ サーバ**」テーブルに変更したプロキシ サーバが表示されます。

ユーザ プロキシ サーバの削除

ウェブ プロキシ サーバを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > ウェブ プロキシ**」ページに移動します。
2. 「**ユーザ プロキシ サーバ**」テーブルで、削除するプロキシ サーバを選択し、「**この登録を削除する**」アイコンの上にマウス ポインタを置きます。
3. 「**この登録を削除する**」を選択します。
4. 「**OK**」を選択します。

すべてのウェブ プロキシ サーバを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > ウェブ プロキシ**」ページに移動します。
2. 「**ユーザ プロキシ サーバ**」テーブルで、見出しの左上のチェックボックスをオンにします。すべてのユーザ プロキシ サーバが選択されます。「**選択した登録をすべて削除する**」を選択します。
3. 「**OK**」を選択します。

7

PortShield グループ

PortShield インターフェースとは、Dell Networking X シリーズ、つまり拡張されたスイッチ上のポートを含む、一連のポートが割り当てられた仮想インターフェースです。PortShield 手法により、LAN ポートの一部または全部を別々のセキュリティ コンテキストに設定し、WAN と DMZ からだけでなく、ネットワーク内の機器間でも保護できるようになります。実際、各コンテキストには、専用の精密パケット検査ファイアウォールによって保護されるワイヤスピード PortShield があります。「**ネットワーク | システム > PortShield グループ**」ページで、ポートを手動でグループ化すると、それらのポートで共通のネットワーク サブネットおよび共通のゾーン設定を共有できます。

ヒント: PortShield グループを使用しなくても、「**ネットワーク | システム > インターフェース**」ページで複数のインターフェースにいつでもゾーンを適用できます。ただし、PortShield を使用してグループ化しないと、それらのインターフェースで同じネットワーク サブネットは共有されません。

PortShield インターフェースには、さまざまな組み合わせのポートを割り当てることができます。PortShield インターフェースに割り当てられていないポートはすべて、LAN インターフェースに割り当てられます。

補足: TZ シリーズ ファイアウォールは Dell Networking X シリーズ スイッチおよび Dell Networking X シリーズ ソリューションをサポートしており、それによりファイアウォールの機能、特にポートシールド インターフェースの機能が拡張されます。「*Dell Networking X シリーズ スイッチの PortShield インターフェースの設定*」を参照してください。

補足: Dell Networking X シリーズ スイッチの PortShield インターフェースの設定についても、「*Dell Networking X シリーズ スイッチの PortShield インターフェースの設定*」を参照してください。

「**ネットワーク | システム > PortShield グループ**」では、PortShield インターフェースへのポート割り当てを以下の方法で管理できます。

- ポート画像
- ポート構成
- 外部スイッチ構成
- 外部スイッチ診断

静的モードとトランスペアレント モード

PortShield インターフェースの作成に使用できる IP 割り当て方式は 2 種類あります。

- 静的モード
- トランスペアレント モード

静的モードの処理

静的モードで PortShield インターフェースを作成する場合、PortShield インターフェースに適用する明示的アドレスを手動で作成します。そのインターフェースに割り当てるポートはすべて、このアドレスで識別されます。静的モードは、保護ゾーン、公開ゾーン、または無線ゾーンに割り当てられるインターフェースに使用できます。

補足: 静的モードで PortShield インターフェースを作成する場合、そのインターフェースに割り当てる IP アドレスが別の PortShield インターフェースに使用されていないことを確認してください。

トランスペアレント モードの処理

トランスペアレント モードのアドレス指定では、アドレス オブジェクトの割り当てを通じて、現在のインターフェースで WAN サブネットワークを共有できます。インターフェースの IP アドレスは、WAN インターフェースの IP アドレスと同じになります。トランスペアレント モードは、保護ゾーンと公開ゾーンに割り当てられるインターフェースに使用できます。

補足: PortShield インターフェースに割り当てる IP アドレスが WAN サブネットワーク内にあることを確認してください。

トランスペアレント モードで PortShield インターフェースを作成する場合、PortShield インターフェースに適用するアドレスの範囲を作成します。これらのアドレスは、アドレス オブジェクトという 1 つのエンティティに含めます。アドレス オブジェクトを使用することで、一度定義したエンティティを SonicOS インターフェース全体の複数の参照インスタンスで再利用することができます。アドレス オブジェクトを使用して PortShield インターフェースを作成する場合、そのインターフェースに割り当てられるポートはすべて、アドレス範囲で指定するアドレスのいずれかによって識別されます。

補足: 静的にアドレス指定する PortShield インターフェースは、それぞれ 1 つのサブネットワークに作成する必要があります。複数のサブネットワークに PortShield インターフェースを分散させることはできません。

SonicOS がサポートする X シリーズ/N シリーズ スイッチ

トピック:

X シリーズ/N シリーズ ソリューションについて

ファイアウォール、スイッチなどの重要なネットワーク要素は、一般に個別に管理する必要があります。SonicOS により、装置の管理インターフェースと GMS を使用して、ファイアウォールとスイッチを一元的に管理できます。

SonicWall セキュリティ装置で使用可能なインターフェースの最大数は、モデルによって異なります。この機能は、SonicOS を実行するすべての SonicWall ファイアウォールでサポートされます

- (NSsp 12000 シリーズを除く)。
- NSA 2600

ある種の配備では、ファイアウォール上で使用可能なインターフェースの最大数を軽く超えるポート数が必要になる場合があります。X シリーズ/N シリーズ ソリューションでは、スイッチ上のポートを装置の拡張インターフェースと見なすことができます。そのため、使用できるインターフェースの数を最大 192 (スイッチによって値は異なる) に増やすことができます。これらの拡張ポートは、Portshield で保護したり、高可用性 (HA) を提供するように設定したり、装置の他のインターフェースとして扱われるようにすることができます。

性能の要件

SonicWall 装置は次のことができるようになりました。

- 最大 4 台のスイッチをプロビジョニングする。
- より多くのポートを管理する。

X シリーズ/N シリーズ スイッチでサポートされる主な機能

ⓘ **補足:** これらの機能の詳細は、『*SonicWall SonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』を参照してください (サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation//) の「**製品を選択します**」フィールドで「**TZ シリーズ**」を選択します)。

- X シリーズ/N シリーズ スイッチの拡張スイッチとしてのプロビジョニング
- PortShield 機能
- 拡張スイッチ インターフェース設定の実行
- 基本的な拡張スイッチ グローバル パラメータの管理
- GMS による拡張スイッチの管理
- PortShield 機能を伴った高可用性 (HA)

  HA モードにおける PortShield 機能が共通アップリンクを使用してサポートされます。この設定では、アクティブ/スタンバイ装置とスイッチの間のリンクが、すべての PortShield トラフィックを伝送する共通アップリンクとして機能します。また、この設定では、PortShield ホストとして機能する装置インターフェースが、アクティブ装置とスタンバイ装置に接続された同じスイッチではなく、独立したスイッチに接続されている必要があります。これにより、同じ PortShield VLAN でのパケットのループが回避されます。PortShield メンバーは、アクティブ/スタンバイ装置から制御されるスイッチのポートに接続できます。
- 拡張スイッチの診断サポート
- SPM による共通アップリンク設定での VLAN のサポート

- 専用アップリンク設定での VLAN のサポート
- VLAN トラフィック用の共通アップリンクを介した一元管理

  VLAN は共通アップリンクでもサポートされます。このため、装置とスイッチを結ぶ単一のリンクで、スイッチを管理する装置の管理トラフィック、セキュリティ装置のインターフェースに対応する IDV (Interface Disambiguation via VLAN) VLAN の PortShield トラフィック、および共通アップリンク インターフェースに存在する VLAN サブインターフェースのトラフィックを伝送できます。

  ⓘ **補足:** 同じスイッチに対する専用アップリンクまたは共通アップリンクとして設定されたセキュリティ装置インターフェースに、重複する VLAN が存在することはできません。これは、VLAN 空間がスイッチ上でグローバルだからです。

  ⓘ **補足:** アクセス/トランク設定用の VLAN を選択せずに、拡張スイッチ インターフェースから共通アップリンク インターフェースへの PortShield を設定することはできません。
- 特定の X シリーズ/N シリーズ スイッチが備えている装置向けの PoE/PoE+ 機能および SFP/SFP+ 機能
- 設定メッセージのバッチ化 – X シリーズ/N シリーズ スイッチのサポートを容易にするため、設定メッセージをバッチ化してからスイッチに送信できます。

PortShield 機能と X シリーズ/N シリーズ スイッチ

PortShield アーキテクチャは、装置のポートを複数の独立したセキュリティ ゾーンに設定することを可能にします。ゾーンをまたいでデバイス間を流れるトラフィックを精密パケット検査セキュリティ装置で保護できます。PortShield 機能の詳細については、「PortShield インターフェースの設定」を参照してください。

SonicWall X シリーズ/N シリーズ ソリューションでは、拡張スイッチ上で装置インターフェースに対するポートシールド機能を使用できます。X シリーズ/N シリーズ スイッチは L2 スイッチで、既定では拡張スイッチのすべてのポートが既定の VLAN 1 のアクセス ポート部として設定されます。拡張スイッチのポートを装置インターフェースに対してポートシールドすると、それらのポートは PortShield VLAN に対応する VLAN のアクセス ポートとして再設定されます。このような設定は、PortShield ホスト インターフェースの IDV VLAN とも呼ばれます。

PortShield によるさまざまなトラフィック シナリオ

- ネットワーク装置を同一の PortShield グループに属する、拡張スイッチのポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックは拡張スイッチによって自動的に交換されます。
- ネットワーク装置を拡張スイッチのポートに接続し、さらに同一の PortShield グループに属する、セキュリティ装置のポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはセキュリティ装置の内部スイッチによって交換されます。
- ネットワーク装置をセキュリティ装置のインターフェースに向けられる、拡張スイッチのポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはソフトウェア内のデータ パスで処理されます。これらのトラフィックをセキュリティ装置のセキュリティ サービス (アクセス ルール、精密パケット検査、侵入防御など) で処理することもできます。
- ネットワーク装置を拡張スイッチのポートに接続し、さらに異なるゾーンまたは異なる PortShield グループに属する、セキュリティ装置のポートに接続した場合、それらのネットワーク装置の間を流れるトラフィックはソフトウェア内のデータ パスで転送されます。それらのトラフィックはセキュリティ装置のセキュリティ サービスによってソフトウェアで処理されます。

X シリーズ/N シリーズ スイッチをポート シールド するための前 提条 件

ⓘ **重要:**トポロジに複数の 2 台以上のスイッチがある場合は、それらのスイッチをカスケード接続またはデイジーチェーン接続にすることができます。つまり、1 台のスイッチを、装置に接続されている別のスイッチに接続できます。

X シリーズ スイッチ (モデル X1052/X1052P 以外) は、スイッチへの不正アクセスを防止するために非管理モードで出荷されます。スイッチを管理モードに切り替えるには、電源プラグ近くの「モード」を 7 秒以上押す必要があります。

出荷時のモデル X1052/X1052P は既定で管理モードになっています。

スイッチの初期セットアップ段階では、装置のインターフェースで DHCP サーバが有効になっていても X シリーズ スイッチの IP が動的に変化しないようにするために、動的 IP ではなく静的 IP を選択してください。

これらの機能の詳細は、『*SonicWall SonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』を参照してください (サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation//) の「**製品を選択します**」フィールドで「**TZ シリーズ**」を選択します)。

- 初期の IP アドレス、ユーザ名/パスワード設定 (スイッチに記載されている) は別として、その他の設定は X シリーズ スイッチの GUI/コンソールから直接行わないようにすることをお勧めします。そのようにすると、装置と X シリーズ スイッチの設定状態との同期がとれなくなります。
- X シリーズ スイッチを装置から管理するには、装置のインターフェースの 1 つが X シリーズ スイッチと同じサブネットに存在する必要があります。例えば、既定の IP `192.168.2.1` を使って X シリーズ スイッチを管理する場合は、装置のインターフェースを `192.168.2.0/24` サブネット内に設定し、X シリーズ スイッチに接続する必要があります。
- 装置からスイッチのプロビジョニングや管理を行う前に、装置から X シリーズ スイッチに Ping を実行して X シリーズ スイッチに到達できることを確認します。
- VLAN サポート:
    - VLAN のサポートは共有された共通のアップリンクで利用できます。例えば、X シリーズ スイッチの共有アップリンクとしてプロビジョニングされている装置インターフェースでは VLAN を設定できません。
    - VLAN サポートの詳細は、『*SonicWall SonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』を参照してください (サポート ポータル (https://www.sonicwall.com/ja-jp/support/technical-documentation//) の「**製品を選択します**」フィールドで「**TZ シリーズ**」を選択します)。専用アップリンクとして設定された複数の装置インターフェースに重複する VLAN は存在できません。例えば、X3 と X5 が専用アップリンクとして設定されている場合、VLAN 100 は X3 と X5 の両方に存在できません。このような設定は拒否されます。

Dell X シリーズ/N シリーズのデイジーチェーン接 続 のサポート

SonicOS X スイッチ/N スイッチ デイジーチェーン接続ソリューションは、デイジーチェーン モードで接続された SonicWall 装置とスイッチとの統合を可能にします。デイジーチェーン モードでは、すべての Dell スイッチ モデルとの統合がサポートされます。

デイジー チェーン接続により、大規模な設備 (倉庫など) を持つユーザは、敷地内に 2 台のスイッチを 1,000 フィート以上の距離を置いて配備できます。2 台のスイッチは光ファイバーを介して相互に接続し、1 台目のスイッチ (親スイッチ) を装置に接続して、両方のスイッチを装置から管理できるようにします。こうした配備では、装置の単一イ

ンターフェースを使用して、スイッチ上のより多くのインターフェースにアクセスすることもできます。親スイッチおよび子スイッチのすべてのインターフェースを装置から管理できます。

トピック:

- 想定条件と依存関係
- デイジー チェーン接続のサポート

想定条件と依存関係

- SonicOS スイッチのデイジーチェーン接続ソリューションでサポート可能なのは、シングル レベルのチェーン接続のみです。2 台を超えるスイッチを直列に接続する、マルチレベルのチェーン接続はサポートされていません。例えば、親スイッチを子スイッチに接続することはできますが、この子スイッチを別の子スイッチに接続することはできません。
- プロビジョニング可能な拡張スイッチは最大 4 台という上限があります。例えば、1 台の親スイッチは最大 3 台の子スイッチを持つことができます。
- デイジーチェーン接続モードでは、子スイッチでサポートされているトポロジが共通アップリンクのみです。このトポロジでは、子スイッチが単一のアップリンクによって親スイッチに接続されます。専用アップリンクや隔離されたリンクなど、その他のバリエーションは子スイッチではサポートされていません。

デイジー チェーン接続のサポート

デイジーチェーン モードで接続された双方のスイッチは同じサブネット内の IP アドレスを持つ必要があり、装置はこのサブネットに到達可能でなければなりません。デイジーチェーン接続モードにあるこれらのスイッチのプロビジョニングの処理は、2 つのステップで行います。

1. 親スイッチをスタンドアロン スイッチとしてプロビジョニングします。
2. 子スイッチをデイジーチェーン接続されるスイッチとしてプロビジョニングします。

PoE/PoE+ および SFP/SFP+ のサポート

SonicWall 装置は PoE/PoE+ 機能をサポートしませんが、特定のスイッチにこの機能を追加することができます。詳細は、「X シリーズ スイッチの PoE/PoE+ および SFP/SFP+ のサポート」を参照してください。この機能を追加すると、SonicWall 装置で使用できる SonicWave が増えます。特に 802.11ac をサポートする新しい SonicWave を使えるのは、大きなメリットです (802.11ac は最大 30 W の電力をサポートしますが、802.11a/b/g/h は最大 15.4 W に留まります)。

一部の X シリーズ スイッチでも、SFP/SFP+ 機能がサポートされています。詳細は「X シリーズ スイッチの PoE/PoE+ および SFP/SFP+ のサポート」を参照してください。

X シリーズ スイッチの PoE/PoE+ ポートの設定は、X シリーズ スイッチの UI から管理できます。SonicWall 装置の「**ネットワーク | システム > Portshield グループ**」では管理できません。

X シリーズ スイッチのモデル	サポートする機能
X1008	1 PoE PD ポート、既定でポート 8 が PD ポート
X1008P	8 PoE ポート、全体で最大 123 W、既定でポート 1 ～ 8 が PoE をサポート
X1018	2 1GbE SFP ポート、既定でポート 17 と 18 が SFP をサポート

X1018P	16 PoE ポート、全体で最大 246W、既定でポート 1 ～ 16 が PoE をサポート 2 1GbE SFP ポート、既定でポート 17 と 18 が SFP をサポート
X1026	2 1GbE SFP ポート、既定でポート 25 と 26 が SFP をサポート
X1026P	24 PoE/12 PoE+ ポート、全体で最大 369W、既定で: • ポート 1 ～ 12 が PoE+ をサポート • ポート 13 ～ 24 が PoE をサポート 2 1GbE SFP ポート、既定でポート 25 と 26 が SFP をサポート
X1052	4 10GbE SFP ポート、既定でポート 49 ～ 52 が SFP+ をサポート
X1052P	24 PoE/12 PoE+ ポート、全体で最大 369W、既定で: • ポート 1 ～ 12 が PoE+ をサポート • ポート 13 ～ 24 が PoE をサポート • ポート 25 ～ 48 は PoE と PoE+ のどちらにも未対応 4 10GbE SFP ポート、既定でポート 49 ～ 52 が SFP+ をサポート
X4012	12 10GbE SFP ポート、既定でポート 1 ～ 12 が SFP+ をサポート

重要: 外部電源のない SonicWave AC の場合、X1026P または X1052P の でポート 1 ～ 12 がポートシールドされている必要があります。
外部電源のない SonicWave の AC 以外のモデルは、ポート 1 ～ 8 (X1008P)、1 ～ 16 (X1018P)、または 1 ～ 24 (X1026P、X1052P) にポートシールドできます。
外部電源のある SonicWave は、どのイーサネット ポートにもポートシールドできます。

X シリーズ/N シリーズ ソリューションと SonicPoint

拡張スイッチのポートは、装置の WLAN ゾーンにポートシールドでき、それらのポートに SonicPoint を接続できます。

SonicPoint を X シリーズ/N シリーズ スイッチに接続するときは SonicPoint の所要電力を考慮することが大切です。SonicPoint ACe/ACi/N2 には、最低 25.5 W が必要です。お使いのスイッチ モデルが PoE+ をサポートしていない場合は、SonicPoint 電力インジェクタを使用する必要があります。スイッチの PoE+ サポート状況については、次を参照してください。「PoE/PoE+ および SFP/SFP+ のサポート」SonicPoint の管理の詳細については、ナレッジベース記事『*SonicWall TZ Series and SonicWall X-Series Solution managing SonicPoint ACe/ACi/N2 access points*』を参照してください。

GMS による拡張スイッチの管理

スイッチの統合機能により、SonicOS 管理インターフェースと SonicWall GMS を使用して装置とスイッチの両方を一元的に管理できます。GMS は、拡張スイッチのプロビジョニング、拡張スイッチ インターフェースの設定、拡張スイッチのグローバル パラメータの管理など、すべての設定操作に対応しています。

詳細については、サポート ポータルにある『GMS 管理ガイド』を参照してください。https://www.sonicwall.com/ja-jp/support/technical-documentation// に移動し、「**製品を選択します**」フィールドで「GMS」を選択します。

拡張スイッチのグローバル パラメータ

「拡張スイッチのグローバル パラメータ」に、SonicOS 管理インターフェースから設定できる拡張スイッチのグローバル パラメータを示します。

これらのパラメータの詳細は、『*SonicWallSonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』を参照してください（サポート ポータル（https://www.sonicwall.com/ja-jp/support/technical-documentation//）の「**製品を選択します**」フィールドで「**TZ シリーズ**」を選択します）。

拡張スイッチのグローバル パラメータ

すべてのスイッチ	X1026P および X1052P のみのスイッチ
STP モード	PoE 警告使用量のしきい値
STP 状況	PoE トラップ
	PoE 電力制限モード

リンクの概要

管理トラフィックのみを伝送する管理（MGMT）リンクは、ポートシールドの対象とすることはできません。

データ リンクは、すべての PortShield トラフィックを伝送します。そのすべての伝送内容がデータなら共通リンクと呼ばれます。多くはありませんがトポロジによっては管理トラフィックを伝送するケースもあり、その場合、共有リンクと呼ばれます。

共有リンクまたは共通リンクは、ポートシールドされたすべてのグループを伝送します。

専用リンクは、1 つの PortShield グループのみを伝送できます。このグループは、装置の専用ポートに対してポートシールドされている必要があります。

アップリンク インターフェースの概要

アップリンク インターフェースは、タグ付けされた / タグ付けされないトラフィックを伝送するように設定された「トランク」ポートとして表示されます。拡張スイッチを追加する際に装置アップリンクと X スイッチ アップリンクのオプションを使うと、SuperMassive アップリンクとして設定された装置のポートと、スイッチ アップリンクとして設定された拡張スイッチのポートが、すべての IDV VLAN についてタグ付けされたトラフィックを送受信するように自動的に設定されます。IDV VLAN のトラフィックがタグ付けされると、ファームウェアは PortShield ホスト インターフェースでこのトラフィックを扱うことができます。

アップリンク インターフェースを設定するための条件

- インターフェースは、物理インターフェースでなければなりません。仮想インターフェースは使用できません。
- インターフェースは、スイッチ インターフェースでなければなりません（一部のプラットフォームでは、装置の一部のインターフェースがスイッチに接続されません。そのようなインターフェースは許可されません）。
- インターフェースを PortShield ホストにすること（他の装置インターフェースをこのインターフェースからポートシールドすること）、または PortShield グループ メンバーにすること（他の装置インターフェースからポートシールドされること）はできません。

- インターフェースは、ブリッジ プライマリ インターフェースまたはブリッジ セカンダリ インターフェースであってはなりません。
- インターフェースは、子を持つことができません（他の子インターフェースの親インターフェースになることはできません）。

ログ記録とSyslog サポート

クリティカルな設定イベント（スイッチの追加/削除、拡張スイッチ ポートでのポートシールドの設定など）やネットワーク イベント（ポートのアップ/ダウンなど）をログに記録するためのサポートが用意されています。

サポートされているトポロジ

ⓘ **重要:** 装置とスイッチの間のインターフェースをセットアップする前に、『*SonicWall SonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』で、これらのトポロジのプロビジョニング、設定、およびセットアップについて理解してください（サポート ポータル（https://www.sonicwall.com/ja-jp/support/technical-documentation//）の「**製品を選択します**」フィールドで「**TZ シリーズ**」を選択します）。

ⓘ **補足:** PortShield インターフェースと X シリーズ/N シリーズ スイッチを設定するための基本的な事項については、「*ポートの管理*」を参照してください。

X シリーズ/N シリーズ スイッチ サポートでサポートされている主なトポロジは次のとおりです。

- 共通アップリンク設定
- 専用アップリンク設定

ⓘ **補足:** 専用リンクに属するポート経由で SonicPoint をポートシールドしなければなりません。

- 共通アップリンクと専用アップリンクによるハイブリッド設定
- 管理トラフィックとデータ トラフィックの両方を伝送する共有リンク設定
- 管理およびデータ用のアップリンクとして隔離されたリンク
- 専用アップリンクによる HA および PortShield 設定
- 共通アップリンクによる HA および PortShield 設定
- SPM 設定による共通アップリンクを持つ VLAN
- 専用アップリンクによる VLAN 設定
- SonicPoint アクセス向けの専用リンク

SonicOS がサポートする N シリーズ スイッチ

トピック:

N シリーズ スイッチについて

SonicOS は、装置やスイッチなどの重要なネットワーク要素を個別に管理します。Dell N シリーズ スイッチと Dell N シリーズ ソリューションにより、装置の管理インターフェースと GMS を使用して、装置と N シリーズ スイッチの両方を一元的に管理できます。ある種の配備では、TZ シリーズ装置上で使用可能なインターフェースの最大数を軽く超えるポート数が必要になる場合があります。Dell N シリーズ ソリューションでは、N シリーズ スイッチのポートを装置の拡張インターフェースと見なすことができるため、使用可能なインターフェースの数が増えます。

N シリーズ スイッチと N シリーズ ソリューションの基本的な違いの 1 つは、装置がスイッチをプログラムする方法です。

- N シリーズ ソリューションでは、セキュリティ装置がスイッチとの間で設定をプッシュ/取得するメカニズムとして XML API が使用されます。
- N シリーズ ソリューションでは、スイッチを設定し、スイッチから設定を取得するメカニズムとして CLI が使用されます。

TZ シリーズ プラットフォームでサポートされる N シリーズ ソリューションの機能は、これらのプラットフォームでサポートされる N シリーズ ソリューションの機能セットと同等であり、Dell X シリーズ スイッチ ソリューションに類似しています。最大で 4 台の N シリーズ スイッチがサポートされます。N シリーズと N シリーズ スイッチの両方が同じファイアウォールに統合されているシナリオでは、最大 4 つの N シリーズ + N シリーズ スイッチを組み合わせてサポートできます。N シリーズ スイッチのデイジーチェーン接続もサポートされています。

以下は、Dell Switch Integration Solution (Dell スイッチ統合ソリューション) の初期フェーズでサポートされる主要な機能セットです。

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

N シリーズ スイッチの設定

工場出荷時の N シリーズ スイッチには、既定で IP アドレスは設定されておらず、DHCP が有効になっています。たとえば、N1524 スイッチを既定の設定で起動した場合:

```
console#show running-config
!Current Configuration:
!System Description "Dell Networking N1524, 6.2.5.3, Linux 3.6.5"
!System Software Version 6.2.5.3
!
configure
stack
member 1 1 ! N1524
exit
interface vlan 1
ip address dhcp
```

```
exit
snmp-server engineid local 800002a203f48e3807701e
exit
console#
```

N シリーズ スイッチの再起動後、Easy Setup Wizard を使用して初期セットアップを設定できます。このウィザードに従うと、初期のスイッチの設定を短時間で遂行してスイッチを起動できます。

ⓘ | **補足:** `Ctrl Z` を入力すると、いつでもセットアップ ウィザードを終了できます。

ⓘ | **ヒント:** セットアップ ウィザードをスキップして、CLI モードに入り、スイッチを手動で設定することもできます。

ⓘ | **重要:** セットアップ ウィザードを実行するには、60 秒以内にこの質問に答える必要があります。
`Would you like to run the setup wizard (you must answer this question within 60 seconds)? (y/n) y`
それ以外の場合、システムは既定のシステム設定を使用して通常どおりの動作を続行します。空のスタートアップ設定でスイッチをリセットして、Dell Easy Setup Wizard を再実行します。

Dell Easy Setup Wizard を使用して N シリーズ スイッチを設定する方法については、ご使用のスイッチの『*Dell 導入ガイド*』を参照してください。

N シリーズ スイッチの、拡張スイッチとしてのプロビジョニング

ⓘ | **補足:** PoE 関連のフィールドは、N シリーズ スイッチの PoE モデルでのみ設定可能です。

スタンドアロン TZ シリーズ システムでは、拡張スイッチのプロビジョニングは、次の拡張スイッチ パラメータを指定します。

必須パラメータ		オプション パラメータ	
• ID	• ユーザ名	• ファイアウォール アップリンク	• PoE 使用量しきい値
• スイッチ モデル	• パスワード	• スイッチ アップリンク	• PoE 管理モード
• IP アドレス	• スイッチ管理	• STP モード	• PoE 検知種別
		• STP 状況	

高可用性が有効な TZ シリーズシ ステムでは、次の拡張スイッチ パラメータを指定することにより、拡張スイッチを追加できます。

必須パラメータ		オプション パラメータ	
• ID	• ユーザ名	• STP モード	• PoE 使用量しきい値
• スイッチ モデル	• パスワード	• STP 状況	• PoE 管理モード
• IP アドレス	• スイッチ管理		• 検知

ⓘ | **補足:** ファイアウォール アップリンクおよびスイッチ アップリンク パラメータは、高可用性モードで動作している装置には関係ありません。現在、必須パラメータは設定後に変更できません。

アップリンク インターフェースの重要性

アップリンク インターフェースは、タグ付けされた / タグ付けされないトラフィックを伝送するように設定されたトランク ポートとして表示できます。拡張スイッチを追加する際にファイアウォール アップリンクとスイッチ アップリンクのパラメータを使うと、ファイアウォール アップリンクとして設定された装置のポートと、スイッチ アップリンクとして設定された拡張スイッチのポートが、すべての IDV VLAN についてタグ付けされたトラフィックを送受信するように自動的に設定されます。タグ付けされたトラフィックの IDV VLAN は、そのトラフィックに関して SonicOS が受信インターフェース、つまり Portshield ホスト インターフェースを導き出すことができるようにします。

ファイアウォール アップリンクとして設定するインターフェースの要件:

- 物理インターフェースでなければなりません。仮想インターフェースは許可されません。
- スイッチ インターフェースである必要があります (一部のプラットフォームでは、装置の一部のインターフェースがスイッチに接続されません。そのようなインターフェースは除外されます)。
- PortShield ホストにすること (他の装置インターフェースをこのインターフェースからポートシールドすること)、または PortShield メンバーにすること (他の装置インターフェースからポートシールドされること) はできません。
- ブリッジ プライマリ インターフェースまたはブリッジ セカンダリ インターフェースであってはなりません。
- 子を持つことができません (他の子インターフェースの親インターフェースになることはできません)。

N シリーズ スイッチのプロビジョニング

N シリーズ スイッチをプロビジョニングするには、以下の手順に従います。

1. 「**ネットワーク | システム > PortShield グループ | 外部スイッチ構成**」に移動します。
2. 「**+ スイッチの追加**」を選択します。「**スイッチの追加**」ダイアログが表示されます。

3. このスイッチの ID を「**ID**」から選択します。既定値は **1** です。
4. 「**スイッチ モデル**」からスイッチの種別を選択します。

5. 「**一般**」オプションの設定を完了します。

6. 「**詳細**」を選択します。

7. 「**詳細**」オプションを設定します。
   ⓘ | **補足:** PoE オプションは、PoE N シリーズ スイッチに対してのみ表示されます。
8. 「**保存**」を選択します。スイッチは「**外部スイッチの設定**」テーブルに追加されます。

PortShield での拡張スイッチの設定

拡張スイッチを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > PortShield グループ | ポート画像**」に移動します。
2. 設定するポートを選択します。
3. 「**構成**」を選択します。「**スイッチ ポート設定**」ダイアログが表示されます。

4. 以下のオプションを設定します。
5. 「**保存**」を選択します。

ポート画像

「ポート画像」は、装置の PortShield インターフェース（ポート）を表示します。大きな図は、装置の使用可能なインターフェースの構成を表しています。各インターフェースは、その設定状況に応じて色分けされています。

インターフェース構成のカラー コード

色	表しているインターフェースの種別
黒	未定義、つまり PortShield グループに割り当てられていない。
Orange	設定対象として選択されている。
灰色の淡色表示	割り当て不可、つまり PortShield グループに追加済み。
灰色のインターフェースで人の形の図が付いているもの	スイッチ MGMT
上矢印が付いているもの（黒色、オレンジ、灰色を除く）	アップリンク
同じ色（黒色、オレンジ、灰色を除く）	同じ PortShield グループに属し、その色が白色の枠線で囲まれているインターフェースがマスター インターフェース。

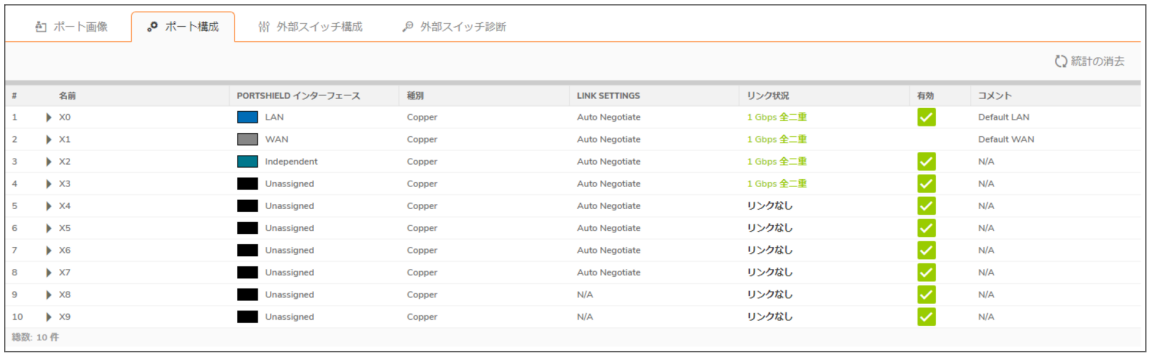
各ポートのグラフィックには対応するポート名 X0 ～ Xn が付いています。特定のインターフェースまたは複数のインターフェースを選択し、「*PortShield グループの設定*」の説明に従って設定できます。

1 つ以上の拡張スイッチがプロビジョニングされると、「**ポート画像**」には、装置とそのスイッチの両方の PortShield インターフェース（ポート）が表示されます。

- 最初のグラフィックには、装置のポートが表示され、ラベルが付いていません。
- 次のグラフィックには、最初の外部スイッチ（外部スイッチ 1）のポートが表示されています。このスイッチは「**SwitchModel 外部スイッチ 1**」（例: X1018P 外部スイッチ 1）とラベル付けされています。
- 外部スイッチがさらにプロビジョニングされた場合、以降のグラフィックには、その他の外部スイッチのポートが ID 順に（外部スイッチ 2、外部スイッチ 3、外部スイッチ 4 のように）表示されます。

外部インターフェースのカラー コード付けは、装置の場合と同じです。次を参照してください。「インターフェース構成のカラー コード」.

ポート構成



「ポート構成」テーブルには、PortShield インターフェースに関する詳細情報が表示されます。

「ポート構成」テーブル

名前	PortShield インターフェースに関連付けられたポート名 (X0、X15 など)。すべての外部スイッチのポートが **ESs:n** の形式で表示されます。ここで、*s* はスイッチ ID、*n* はポート番号をそれぞれ表しています。
PortShield インターフェース	PortShield インターフェースの設定状況と所属 PortShield グループを表す色分けされたグラフィック。このグラフィックは、「**ポート画像**」にある大きな図の縮小版です。
リンク設定	リンク速度: • **自動ネゴシエーション** • **1000Mbps ー 全二重** • **100Mbps ー 全二重** • **100Mbps ー 半二重** • **10Mbps ー 全二重** • **10Mbps ー 半二重**
リンク状況	次のどちらかが表示されます。 • 現在のリンク速度 (緑色)。例: **1000Mbps – 全二重**。 • **接続されていません**。
有効	有効アイコンは色によって状態を示します。 • 緑色 (インターフェースが有効な場合)。 • 淡色表示の灰色 (インターフェースが無効になっている場合)
コメント	インターフェース設定時に入力されたコメント。
構成	次のアイコンがあります。 • **編集** ー 選択時、「**スイッチ ポートの編集**」ダイアログを表示します。このダイアログの詳細は、「**ネットワーク	システム > PortShield グループ**」の「*PortShield インターフェースの設定*」の手順を参照してください。

外部スイッチ構成

ⓘ | **補足:** 外部スイッチがプロビジョニングされていない場合、このテーブルには「***データなし***」と表示されます。

「外部スイッチの設定」テーブル

ID #	外部スイッチの ID 番号: **1**、**2**、**3** または **4**。
モデル	拡張スイッチのモデル番号。
状況	スイッチの状況: 緑色の「**有効**」アイコンは、スイッチが稼働していて使用可能であることを示します。 ⓘ **補足:** 拡張スイッチの電源をオフにしてから装置を再起動 (リブート) した場合、装置が拡張スイッチを検出し、スイッチの「**状況**」を稼働中で使用可能と報告するまでに最大で 5 分かかります。
IP アドレス	拡張スイッチの IP アドレス。
スイッチ モード	スイッチのモード (**スタンドアロン**など)。
スイッチ管理	管理トラフィック用のスイッチ ポート。
ファイアウォール アップリンク	装置のアップリンクとして設定された装置のポート。装置のアップリンクとして設定された装置のポートが存在しない場合は、「なし」と表示されます。
スイッチ アップリンク	スイッチ アップリンクとして設定された拡張スイッチのポート。スイッチ アップリンクとして設定されたスイッチ ポートが存在しない場合は "**なし**" と表示されます。
親スイッチ ID	デイジーチェーン接続されたスイッチにとっての親スイッチの ID。親スイッチとして設定されたスイッチ ポートが存在しない場合、この列には "**該当なし**" と表示されます。
親スイッチ アップリンク	スイッチ アップリンクとして設定された、デイジーチェーン接続されている親スイッチのポート。親スイッチのアップリンクとして設定されたスイッチ ポートが存在しない場合は "**該当なし**" と表示されます。
構成	以下が含まれます。 • 「**編集**」アイコン — 選択すると、「**外部スイッチの編集**」ダイアログが表示されます。 • 「**削除**」アイコン — 選択すると、スイッチ エントリが削除されます。

「**外部スイッチ構成**」では、装置上でプロビジョニングされた外部スイッチに関する情報が提供され、そのスイッチを管理できます。拡張スイッチの設定や削除も行えます。拡張スイッチの設定については、「「PortShield グループ」」を参照してください。拡張スイッチの削除については、『*SonicWall X シリーズ/N シリーズ ソリューション配備ガイド*』を参照してください。

外部スイッチ診断

「外部スイッチ診断」では、以下のことができます。

- 拡張スイッチの再起動
- 拡張スイッチに関する統計の監視
- ファームウェア イメージ、ブート イメージのアップロード

「外部スイッチ診断」は、特定のスイッチに関する統計その他の情報を表示します（一度に表示されるのは 1 つのスイッチに関するもののみ）。既定では、外部スイッチ 1（ES1）のデータが表示されます。2 台以上の外部スイッチがある場合、別の外部スイッチに関するデータを表示するには、「スイッチ名」で「ES2」、「ES3」、または「ES4」を選択します。

スイッチ情報

重要：拡張スイッチの電源をオフにしてから装置を再起動（リブート）した場合、セキュリティ装置が拡張スイッチを検出し、スイッチの「状況」を「**接続**」と報告するまでに最大で 5 分かかります。

外部スイッチを再起動するには、以下の手順を実行します。

1. 「**ネットワーク | システム > PortShield グループ | 外部スイッチ診断**」に移動します。
2. 「**スイッチ名**」で、再起動する外部スイッチを選択します。
3. 「Restart Selected Switch（**選択したスイッチの再起動**）」をクリックします。

統計

すべての統計の現在までの集計は「**統計**」テーブルに表示されます。

統計の収集を最初からやり直す場合は、以下の手順に従います。

1. 「**統計の消去**」を選択してカウンタをリセットします。

「統計」テーブル

名前	ポート名（1 ～ n）。
状況	ポートの状況（「稼働中」または「休止中」）。
受信ユニキャスト パケット	ポートで受信したユニキャスト パケット数。
受信マルチキャスト パケット	ポートで受信したマルチキャスト パケット数。
受信ブロードキャスト パケット	ポートで受信したブロードキャスト パケット数。
受信バイト	ポートで受信したバイト数。

受信エラー	ポートで受信したエラー パケット数。
送信ユニキャスト パケット	ポートで送信したユニキャスト パケット数。
送信マルチキャスト パケット	ポートで送信したマルチキャスト パケット数。
送信ブロードキャスト パケット	ポートで送信したブロードキャスト パケット数。
送信バイト	ポートで送信したバイト数。
FCS エラー	ポートで受信した FCS (frame check sequence) エラー パケット数。
単一衝突フレーム	ポートで検出したフレーム衝突回数。
遅れ衝突	ポートで遅延フレーム ビット送信後に検出されたフレーム衝突回数。
過度の衝突	ポートで再試行回数を超えて検出されたフレーム衝突回数。
内部 MAC 送信エラー	ポートで検出された衝突以外の送信エラー数。
オーバーサイズ パケット	ポートで受信した、想定よりも大きなパケット数。
受信停止フレーム	ポートで受信した停止フレーム数。
送信停止フレーム	ポートで送信した停止フレーム数。

ファームウェア管理

ファームウェア管理」テーブルには、外部スイッチのファームウェアおよびブート コードに関する情報が表示されます。

「ファームウェア管理」テーブル

種別	**ファームウェア**または**ブート コード**。
バージョン	外部スイッチのファームウェアまたはブート コードのバージョン。
作成日	ファームウェアまたはブート コードが作成された日付。
作成時刻	ファームウェアまたはブート コードが作成された時刻。
アップロード	アップロード アイコン。 • 「**ファームウェア**」の場合、「**外部スイッチ ファームウェアのアップロード**」ダイアログが表示されます。 • 「**ブート コード**」の場合、「**外部スイッチ ブート コードのアップロード**」ダイアログが表示されます。

ファームウェアまたはブート コードをアップロードするには、以下の手順を実行します。

1. **ファームウェア**または**ブート コード**の「**アップロード**」をクリックします。「**外部スイッチ ファームウェアのアップロード**」または「**外部スイッチ ブート コードのアップロード**」ダイアログが表示されます。
2. 「**参照**」をクリックします。「**ファイルのアップロード**」ダイアログが表示されます。
3. ファイルを選択します。
4. 「**アップロード**」をクリックします。

PortShield グループの設定

PortShield グループは、SonicOS のさまざまなページで設定できます。

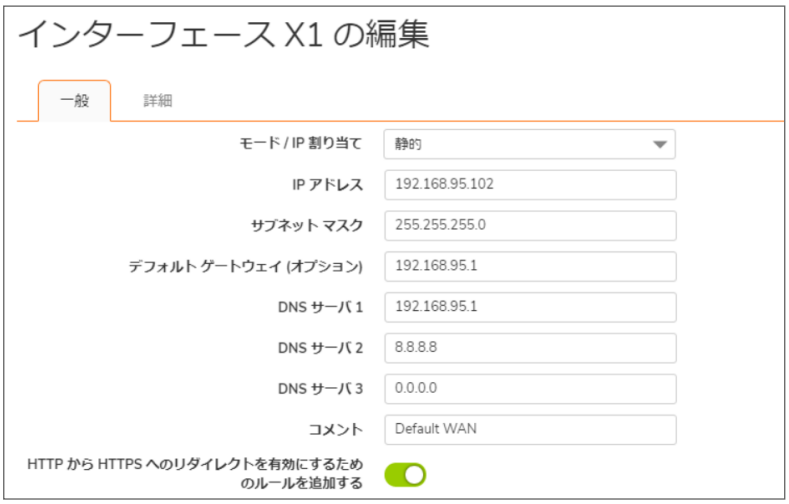
- 「**ネットワーク | システム > インターフェース**」での PortShield インターフェースの設定
- PortShield インターフェース ガイドによる PortShield インターフェースの設定（TZ シリーズ ファイアウォールのみ）
- 「**ネットワーク | システム > PortShield グループ**」での PortShield インターフェースの設定
- 「ポート画像」からの外部スイッチ PortShield グループの設定

「ネットワーク | システム > インターフェース」での PortShield インターフェースの設定

ⓘ **重要:** インターフェースとするポートには IP アドレスを設定してください。設定しないと、そのポートは「**PortShield インターフェース**」に表示されません。

PortShield インターフェースを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > インターフェース**」に移動します。
2. 「**インターフェース設定**」テーブルで、設定するインターフェースの「**この登録を編集する**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。



3. 「**ゾーン**」で、インターフェースを割り付けるゾーン種別オプションを選択します。追加のオプションが表示されます。

ⓘ **補足:** PortShield インターフェースを追加できるのは、**保護**ゾーン、**公開**ゾーン、および**無線**ゾーンのみです。

4. 「**モード/IP 割り当て**」ドロップダウン メニューで、「**PortShield スイッチ モード**」を選択します。再びオプションが変化します。
5. 「**PortShield 先**」で、このポートを割り付けるインターフェースを選択します。選択したゾーンと一致するポー

トのみが表示されます。

6. 「**OK**」を選択します。

PortShield インターフェース ガイドによる PortShield インターフェースの設定 (TZ シリーズ ファイアウォールのみ)

『*SonicOS クイック設定ガイド*』の説明に従って、PortShield インターフェースを *PortShield インターフェース ガイド*によって設定できます。*PortShield インターフェース ガイド*には、次のようにしてアクセスできます。

- 管理インターフェースの任意のページで「**クイック設定ガイド**」を選択します。「**設定ガイド**」が表示されるので、「**PortShield インターフェース ガイド**」を選択します。
- TZ シリーズ セキュリティ装置の「**ネットワーク | システム > インターフェース**」ページで、「**PortShield ウィザード**」を選択して*PortShield インターフェース ガイド*を表示します。

「ネットワーク | システム > PortShield グループ」での PortShield インターフェースの設定

「**ポート画像**」には、PortShield インターフェースの現在の設定を視覚的に表したものが表示されます。グラフィック表示の説明については、「*ポート画像でのインターフェース (ポート) の表示*」を参照してください。

この PortShield グループのグラフィック インターフェースを使用すると、グループ化したいポートを選択することにより、ポートを手動でグループ化できます。ポートをグループ化すると、それらのポートで共通のネットワーク サブネットおよび共通のゾーン設定を共有できます。

ⓘ **補足:** インターフェースを PortShield でグループ化するには、その前にインターフェースを設定しておいてください。

PortShield グループを設定するには、以下の手順を実行します。

1. ポート画像で、PortShield グループに含めたいインターフェースを選択します。選択したインターフェースの色が黄色に変わります。
2. 「**構成**」をクリックします。「**スイッチ ポートの編集**」ダイアログが表示されます。

   ⓘ **補足:** このポートのインターフェースの名前は、淡色表示になっており、変更できません。

3. 「**ポート有効**」で、そのインターフェースを有効にするか無効にするかを選択します。既定では「**有効**」になっています。

4. 「**PortShield インターフェース**」で、この PortShield インターフェースのマスター インターフェースとして割り当てるインターフェースを選択します。既定では「**未定義**」になっています。

   ⓘ | **補足:** 外部スイッチ ポートでは PortShield オプションが無効になることがあります。

5. 「**リンク速度**」で、そのインターフェースのリンク速度を選択します。
   - **自動ネゴシエート**（既定）
   - **1000 Mbps ー 全二重**
   - **100 Mbps ー 全二重**
   - **100 Mbps ー 半二重**
   - **10 Mbps ー 全二重**
   - **10 Mbps ー 半二重**
6. 「OK」をクリックします。

「ポート画像」からの外部スイッチ PortShield グループの設定

ⓘ | **重要:** 拡張スイッチの電源をオフにしてから装置を再起動（リブート）した場合、セキュリティ装置が拡張スイッチを検出し、スイッチの「**状況**」を「**接続**」と報告するまでに最大で 5 分かかります。
拡張スイッチを PortShield グループに設定すると、この設定が「**ネットワーク | システム > PortShield グループ**」に表示されるまで最大で 5 分かかります。

ⓘ | **重要:** インターフェースを PortShield でグループ化するには、その前にインターフェースを設定しておいてください。

ⓘ | **補足:** 詳細については、https://www.sonicwall.com/support/technical-documentation/ にアクセスして『*SonicWall SonicOS X シリーズ/N シリーズ ソリューション配備ガイド*』（「製品を選択します」フィールドで NSa シリーズおよび TZ シリーズを選択）を参照してください。

「**ネットワーク | システム > PortShield グループ**」には、セキュリティ装置と拡張（外部）スイッチの双方の PortShield インターフェースの現在の設定がグラフィック表現で表示されます。外部スイッチが 1 台ならグラフィックは 2 つ、外部スイッチが 2 台ならグラフィックは 3 つ、というように表示されます。各スイッチのグラフィックには、スイッチのモデルと外部スイッチ ID（1、2、3、4）が表示されます。

この PortShield グループのグラフィック インターフェースでは、グループ化したいポートをクリックすることにより、セキュリティ装置およびスイッチのポートを手動で一緒にグループ化できます。ポートをグループ化すると、それらのポートで共通のネットワーク サブネットおよび共通のゾーン設定を共有できます。

外部スイッチで PortShield グループを設定するには、以下の手順を実行します。

1. 「**ネットワーク | システム > PortShield グループ**」で、「PortShield インターフェースの設定」の手順に従って装置のポートを設定します。
2. 外部スイッチのポート画像内で、PortShield グループに含めたいインターフェースを選択します。選択したインターフェースの色が黄色に変わります。
3. 「**構成**」をクリックします。「**複数のスイッチ ポートを編集する**」ダイアログが表示されます。

「**名前**」フィールドは淡色表示になっており、変更できません。ここには、装置のポートと選択した外部スイッチのポートの両方の名前が表示されます（n は選択したポート）。

- ファイアウォールのポートの名前は、**Xn** となっています。
- 外部スイッチ 1 のポートは、**ES1 : n** となります。
- 外部スイッチ 2 のポートは、**ES2: n** となります。
- 外部スイッチ 3 のポートは、**ES3 : n** となります。
- 外部スイッチ 4 のポートは、**ES4 : n** となります。

6. 「**ポート有効**」で以下の選択を行います。

- **無効**
- **有効**
- **—現在の設定を保持する—**（既定）— 既定では、拡張スイッチのすべてのポートが有効になります。

5. 「**PortShield インターフェース**」で、これらの PortShield インターフェースのマスター インターフェースとして割り当てるインターフェースを選択します。

- **未定義**
- **ポート名**

ⓘ **重要 :** インターフェースとするポートには IP アドレスを設定してください。設定しないと、そのポートは「PortShield インターフェース」に表示されません。

- **—現在の設定を保持する—**（既定）

ⓘ **補足:** 外部スイッチ ポートでは PortShield オプションが無効になることがあります。ここでポートシールドしたポートは、対応する PortShield VLAN の VLAN にアクセスしたとき自動的に設定されます。

6. 「**リンク速度**」で、そのインターフェースのリンク速度を選択します。

- **自動ネゴシエート**
- **1000 Mbps — 全二重**
- **100 Mbps — 全二重**
- **100 Mbps — 半二重**
- **10 Mbps — 全二重**
- **10 Mbps — 半二重**
- **—現在の設定を保持する—**（既定）— 既定では、拡張スイッチのすべてのポートのリンク速度は、**自動ネゴシエート**に設定されます。

7. 「**OK**」をクリックします。

8

VLAN 変換

トピック:

VLAN 変換（割付）機能を使用すると、VLAN に到着したトラフィックを保護モードで動作しているワイヤ モード インターフェースへ送るとき、そのトラフィックをペアになっている送信側インターフェースの別の VLAN に割り付けることができます。装置に送られてきたトラフィックのルートを変更して異なる VLAN へ送ることで、詳細な分析や加工、あるいはトラフィックの単なる再割付を行うことができます。この機能は、ワイヤ モード対応のすべての機器でサポートされています。

ワイヤ モードの利点は、VLAN 割付を事前にプロビジョニングできることです。これにより、インターフェースがトラフィックを受け取る前に割付を用意できます。アクティブなワイヤ モード インターフェース上で割付を追加または削除することもできます。

ⓘ | **補足:** VLAN 変換は、ワイヤ モードをサポートするすべてのプラットフォームで使用できます。

ⓘ | **補足:** VLAN 変換と VLAN インターフェース越しのワイヤ モードを同時に有効にすることはできません。

割付のモード

VLAN 割付は以下のモードで作成できます。

- **単方向割付** — 例えば、次のようなケースがあります。
  - 安全性の低いネットワークから安全性の高いネットワークに対して保護された印刷を行う。
  - 安全性の低いネットワークから安全性の高いネットワークに対してアプリケーションやオペレーティング システムのアップデートを転送する。
  - SOC（セキュリティ オペレーション センター）で複数ネットワークを監視する。
  - 安全性の高いネットワークで時間同期機能を提供する。
  - ファイルを転送する。
  - 安全性の低いネットワークから安全性の高いネットワークに対して "メール受信" 通知を行う。
- **双方向割付** — 例えば、装置経由で機器とやり取りする双方向接続（TCP など）をセットアップする場合に使います。

割付の恒久性

インターフェース ペアに対して作成した VLAN 割付は、設定の一部として格納され、再ロード後も持続します。ワイヤ モード ペア（保護モード）にそれらと関連付けられた割付がある場合、割付ポリシーが削除されない限り、ワイヤ モードを変更できません。

複数のインターフェース ペアの割り付け

複数のインターフェース ペアに対して同時に VLAN 割付を作成できます。これらのインターフェースは、VLAN 割付の作成時に既存の保護ワイヤ モード ペアの一部を形成していなければなりません。複数のインターフェースを持つインターフェースに対して割付を作成することもできます。ただし、どの時点でも現在アクティブなワイヤ モード ペアの割付だけが使われます。

ペアになっているインターフェースが変更された場合、「インターフェースにワイヤモード VLAN 登録がある場合、ワイヤモード ペア インターフェースを変更することはできません」というメッセージが表示されます。

例

複数のインターフェース ペアの割り付け

「複数のインターフェース ペアの割り付け」を見ると、X12 から X13 への割付（ポリシー 1）と X12 から X15 への割付（ポリシー 2）があります。

現在、X12 と X13（ポリシー 1 および 3）、X14 と X15（ポリシー 4 および 6）だけがワイヤ モード ペアを形成しており、「アクティブ」列の緑色のチェックマークが示すように、ポリシー 1、3、4、および 6 だけがアクティブになっています。

ⓘ **補足:** インターフェースにワイヤ モード VLAN 登録が存在する場合は、ワイヤ モード ペア インターフェースを変更できません。

VLAN 割付の作成と管理

トピック:

- VLAN 割付の作成
- VLAN 割付の管理

「**ネットワーク | システム > VLAN 変換**」で、インターフェースの VLAN 割付を作成、管理することができます。

追加アイコン	「**VLAN 変換の追加**」ダイアログを表示します。
削除	「**削除**」ドロップダウン メニューを表示します。 • **選択項目の削除** • **すべて削除**
検索フィールド	関心のある VLAN 変換だけを表示できます。
再表示アイコン	「VLAN 変換」テーブルを再表示します。

ポリシー番号とチェックボックス	ポリシーの番号とそれに対応するチェックボックス。
受信インターフェース	受信インターフェースの名前。
受信 VLAN	受信インターフェースの VLAN タグ。
送信インターフェース	トラフィックの割り付け先のインターフェースの名前。
送信 VLAN	トラフィックの割り付け先のインターフェースの VLAN タグ。
逆変換	割付が単方向か双方向かを示します。 • **無効** — 単方向。列は空白です。 • **有効** — 双方向。緑色のチェックマークが表示されます。
動作	割り付けられたペアの状況。 • **アクティブ** — このワイヤ モード ペアは割り付け済みで、アクティブです。緑色のチェックマークが表示されます。 • **非アクティブ** — このワイヤ モード ペアは割り付け済みですが、アクティブでありません（事前プロビジョニング）。列は空白です。
構成	割り付けられたペアの「**編集**」アイコンと「**削除**」アイコンを表示します。

VLAN 割付の作成

単方向 VLAN 割付は、ワイヤ モード ペアの作成前または作成後に作成できます。VLAN 割付の作成は次の 2 ステップで行われます。

1. ワイヤ モード ペアを保護モードで作成する
2. VLAN 割付を作成する

ワイヤ モード ペアを保護モードで作成する

ワイヤ モード ペアを保護モードで作成するには、以下の手順を実行します。

1. 「**ネットワーク | システム > インターフェース**」に移動します。

2. ワイヤ モード ペアの一方とするインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
3. ワイヤ モード ペアのゾーンを「**ゾーン**」から選択します。オプションが次のように変化します。
4. 「**モード / IP 割り当て**」から「**ワイヤ モード (2 ポート ワイヤ)**」を選択します。再びオプションが変化します。

5. 「**ワイヤ モード種別**」から「**保護 (直列トラフィックのアクティブ DPI)**」を選択します。
6. 現在のインターフェースとペアにするインターフェースを「**ペア インターフェース**」ドロップダウン メニューから選択します。

   ⓘ | **ヒント:** ペアにするインターフェースは未割り当てでなければなりません。
7. ペアにするインターフェースのゾーンを「**ペア インターフェース ゾーン**」から選択します。既定は **LAN** です。
8. 通常のワイヤ モード ペアと同じように他のオプションを設定します (「ワイヤ モードとタップ モードの設定」を参照)。
9. 「**OK**」を選択します。「**ネットワーク | システム > インターフェース**」ページが更新されます。

VLAN 割付を作成する

VLAN 割付を作成するには、以下の手順を実行します。

1. 「**ネットワーク | システム > VLAN 変換**」に移動します。
2. 「**+ 追加**」を選択します。「**VLAN 変換の追加**」ダイアログが表示されます。
3. ペアのうち、トラフィックを受け取る側のワイヤ モード インターフェースを「**受信インターフェース**」から選択します。
4. 「**受信 VLAN**」に、割り付けるトラフィックを受け取る側の VLAN を設定します。
5. ペアのうち、トラフィックを割り付ける対象となるワイヤ モード インターフェースを「**送信インターフェース**」ドロップダウン メニューから選択します。
6. 「**送信 VLAN**」に、トラフィックを割り付ける対象となる VLAN を設定します。
7. 作成する割付のモードに応じて、以下の作業を行います。

- 単方向割付を作成する場合は、「**逆変換**」をオフにします。例えば、インターフェース A の VLAN X をインターフェース B の VLAN Y に割り付ける場合がこれに該当します。

  ⓘ | **補足:** このオプションは、既定では選択されています。
- 双方向割付を作成する場合は、「**逆変換**」をオンにします。例えば、インターフェース B の VLAN Y をインターフェース A の VLAN X に割り付け、さらにインターフェース A の VLAN X をインターフェース B の VLAN Y に割り付ける場合がこれに該当します。

8. 「**追加**」を選択します。「**ワイヤ モード VLAN 変換**」テーブルが更新されます。

VLAN 割付の管理

トピック:

- 割付の編集
- 割付のフィルタリング
- 割付の削除

割付の編集

割付を編集するには、「**設定**」列の対応する「**編集**」アイコンを選択します。「**VLAN 変換の編集**」ダイアログが表示されます。割付に関しては「**逆変換**」以外のすべての設定を変更できます。

割付のフィルタリング

多数の VLAN 割付がある場合、次の操作によって、興味のある割付だけを表示できます。

1. 「**検索**」フィールドにインターフェース名または VLAN タグを入力します。
2. Enter キーを押します。

検索条件を満たす割付だけが表示されます。

すべての割付を再表示するには、以下の手順に従います。

1. 「**検索フィールド**」の条件を削除します。
2. Enter キーを押します。

割付の削除

割付を削除するには、以下の手順に従います。

1. 削除するには:
   単一の割付を削除する場合:
   - 「**設定**」列の対応する「**削除**」アイコンを選択します。

     確認メッセージが表示されます。
   - 対応する「**選択**」チェックボックスを選択したうえで「**削除**」ドロップダウン メニューから「**選択項目の削除**」を選択します。

     確認メッセージが表示されます。
   - 複数の割付を削除する場合は、対応するそれぞれの「**選択**」チェックボックスを選択したうえで「**削除**」ドロップダウン メニューから「**選択項目の削除**」を選択します。

     確認メッセージが表示されます。
   - すべての割付を削除する場合は、「**すべて削除**」ドロップダウン メニューから「**選択項目の削除**」を選択します。

     確認メッセージが表示されます。
2. 「OK」を選択します。

双方向のポリシーでは、一方を削除すると両方の方向が削除されます。

9

IP ヘルパー

IP ヘルパーの使 用

トピック:

IP ヘルパーについて

ⓘ **重要:** WAN インターフェースおよび NAT 向けに構成されたインターフェースについては、IP ヘルパーではサポートしていません。

UDP (ユーザ データグラム プロトコル) の多くは、それぞれのサーバを探し出すためにブロードキャスト/マルチキャストを使用します。この際、通常はサーバが同じブロードキャスト サブネット上に存在する必要があります。サーバがクライアントと異なるサブネット上に存在する状況に対応するためには、UDP ブロードキャスト/マルチキャストをサーバのサブネットに転送するメカニズムが必要になります。このメカニズムを、UDP ブロードキャストの転送と呼びます。IP ヘルパーを使用すると、ブロードキャスト/マルチキャスト パケットが装置のインターフェースを通過し、ポリシーに基づいて他のインターフェースに転送されるようになります。IP ヘルパーを使用して、装置がそのインターフェース上で受信した DHCP 要求を中央の DHCP サーバに転送するように設定できます。

IP ヘルパーは、ユーザ定義のプロトコルと拡張ポリシーをサポートします。また、既存の NetBIOS/DHCP リレー アプリケーションをより細かく制御できるようになりました。拡張された組み込みアプリケーションの一部を以下に示します。

拡張されたビルトイン リレー アプリケーション

プロトコル	UDP ポート番号
DHCP	67/68
DHCPv6	546、547
Net-BIOS NS	137
Net-BIOS データグラム	138
DNS	53
Time サービス	37
Wake on LAN (WOL)	
mDNS	5353 マルチキャスト アドレス: `224.0.0.251`

VPN トンネル インターフェースによる IP ヘルパーのサポート

VPN トンネル インターフェースで IP ヘルパーをサポートできます。「トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ」は、IP ヘルパー内の DHCP リプレイの簡単な例を示しています。

- PC は、DHCP プロトコルから IPv4 アドレスを取得するために必要な機器です。
- ゲートウェイ A は、ゲートウェイに対応した IP ヘルパーです。
- ゲートウェイ B は、DHCP サーバを備えたゲートウェイです。

トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ

VPN トンネル インターフェースを使用して IP ヘルパーを設定するには、以下の手順に従います。

ⓘ **補足:** 「トンネル インターフェース サポートを使用した IP ヘルパー内の DHCP リプレイ」の数字は、タスクの番号に対応しています。

1. PC:
    a. ゲートウェイ A の LAN (X0) サブネットに接続します。
    b. DHCP モード経由で IP アドレスを取得するように設定します。
2. ゲートウェイ A とゲートウェイ B の間の VPN トンネルの設定
    a. VPN トンネル インターフェースを追加します。

3. ゲートウェイ B:
    a. トンネル インターフェースの IP アドレスからゲートウェイ A の X0 インターフェースへのルート登録を追加します。
    b. トンネル インターフェースの発信インターフェースを追加します。
    c. PC の DHCP スコープとして IP アドレス範囲を追加します。
4. ゲートウェイ A:
    a. IP ヘルパーを有効にします。
    b. X0 からゲートウェイ B のトンネル インターフェース アドレスへの IP ヘルパー DHCP リレー プロトコルを追加します。プロトコルは DHCP です。

DHCPv6 リレー

トピック:

- DHCPv6 リレーについて
- DHCPv6 リレーの設定

DHCPv6 リレーについて

SonicOS では、DHCPv6 リレーがサポートされます。DHCP リレー エージェントは、クライアントとサーバ間で DHCP メッセージをやり取りするための仲介ノードとして機能し、クライアントと同じリンク上に存在します。クライアントとサーバが同じ IPv6 リンク上にない場合に、DHCPv6 リレー エージェントを使用して、クライアントとサーバ間でメッセージをリレーします。DHCPv6 リレー エージェントの動作をクライアントから意識する必要はありません。

SonicOS では、サポートされる送信先アドレスに、グローバル アドレスまたはリンクローカル アドレスを指定できますが、マルチキャスト アドレスは使用できません。

DHCPv6 リレーは、物理と仮想の両方のインターフェースで有効にすることができます。DHCPv6 は、IP ヘルパーのプロトコルに組み込まれたアプリケーションの一種です。

DHCPv6 リレーの設定

DHCPv6 リレーを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」ページに移動します。

2. 「**ポリシー**」ビューを選択します。
3. 「**+ 追加**」を選択します。「**IP ポリシーの追加**」ダイアログが表示されます。

4. 「**プロトコル**」から「**DHCPv6**」を選択します。
5. 「**送信元**」から目的のインターフェースを選択します。
6. 「**送信先**」フィールドに、送信先の IPv6 アドレスを入力します。これには、ユニキャスト アドレス、または選択した他のアドレスなど、送信先アドレスのリストを指定することもできます。このアドレスとしてマルチキャスト アドレスを指定することはできません。
7. 「**送信先**」フィールドの送信先が
   - グローバル アドレスの場合は、送信インターフェースを選択する必要はありません。ステップ 8 に進みます。
   - リンクローカルアドレスの場合は、「**送信インターフェース**」から送信インターフェースを選択します。
8. 「**保存**」を選択します。

   クライアントがサーバから新しい IP アドレスを取得すると、このページの「**DHCPv6 リレー リース**」セクションに新規の DHCP リースが表示されます。

IP ヘルパー設定

トピック:

- リレー プロトコル
- ポリシー
- DHCP/DHCPv6 リレー リース

リレー プロトコル

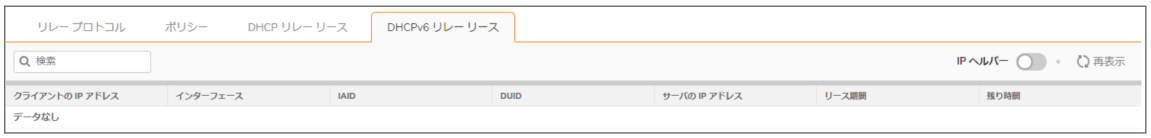
名前	IP ヘルパー アプリケーション名。
ポート	IP ヘルパー アプリケーションの最初の UDP ポート番号。
ポート	IP ヘルパー アプリケーションの 2 番目の UDP ポート番号 (オプション)。
Raw	IP ヘルパー アプリケーションの設定時に Raw モードが選択されたかどうかを示します。このオプションが有効になっている場合、タイムアウトは無視されます。
プロトコル	UDP。
タイムアウト (秒)	IP ヘルパー キャッシュのタイムアウト時間。「**該当なし**」は Raw モードが選択されていてタイムアウトが無視されることを示します。
モード	プロトコルがサポートしているモードを示します。 • **ブロードキャスト** • **マルチキャスト** • **両方**
マルチキャスト IP	プロトコルが使用するマルチキャスト IP。
IP 変換	IP ヘルパー ポリシーによるパケット転送時に送信元 IP アドレスが変換される

	かどうかを示します。
有効	IP ヘルパー ポリシーが有効かどうかを示します。
構成	エントリの**統計**アイコン、**編集**アイコン、**削除**アイコンがあります。 ⓘ | **補足:** ユーザによって生成されたリレー プロトコルのみを削除できます。

ポリシー

リレー プロトコル	ポリシーのプロトコル。
送信元	ポリシーのインターフェースまたはゾーン。
送信先	ネットワーク送信先。
コメント	ポリシー設定時に入力されたコメント。
有効	IP ヘルパー ポリシーが有効かどうかを示します。
構成	エントリごとに**編集**アイコンと**削除**アイコンがあります。

DHCP/DHCPv6 リレー リース



クライアントの IP アドレス	クライアント機器の IP アドレス。
インターフェース	装置上の受信インターフェース。
DHCP リレー リース:	
• **クライアントの MAC アドレス**	クライアント機器の MAC アドレス。
• **クライアントのベンダー**	クライアント機器の製造元。
DHCPv6 リレー リース	
• **IAID**	インターフェース ID (Interface Association Identifier)。このインターフェースと 1 つ以上の IP アドレスとの間のバインディングです。
• **DUID**	デバイス (ホスト) ID。DHCP 参加者を一意に識別する DHCP UID。

サーバの IP アドレス	DHCP サーバの IP アドレス。
リース期間	リレー リースの期間。
残り時間	リレー リースの残り時間。

DHCP リレー リース テーブルを再表示するには、以下の手順に従います。

1. 「**再表示**」を選択します。

IP ヘルパーの設定

トピック:

- IP ヘルパーの有効化
- リレー プロトコルの管理
- IP ヘルパー ポリシーの管理

IP ヘルパーの有効化

IP ヘルパー機能を有効化するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 「**IP ヘルパー設定**」で「**IP ヘルパーを有効にする**」を選択します。

リレー プロトコルの管理

トピック:

- ユーザ定義リレー プロトコルの追加
- ユーザ定義プロトコルの削除

ユーザ定義リレープロトコルの追加

リレープロトコルを追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 「**リレープロトコル**」ビューの「**+ 追加**」を選択します。「**リレープロトコルの追加**」ダイアログが表示されます。

3. 「**アプリケーションを有効にする**」を選択して、IP ヘルパー アプリケーションを有効にします。
   ⓘ | **補足:** このオプションが無効になっている場合、すべての IP ヘルパー キャッシュが削除されます。
4. 「**名前**」フィールドに、IP ヘルパー アプリケーションの一意の名前（大文字と小文字の区別があります）を入力します。
5. 「**ポート 1**」フィールドに、アプリケーションの一意の UDP ポート番号を指定します。
6. オプションで、「**ポート 2**」フィールドに、一意となる第 2 の UDP ポート番号をアプリケーションに対して指定します。
7. オプションで、「タイムアウト」フィールドに、IP ヘルパー キャッシュ タイムアウトの秒数を 10 ～ 60 の範囲で 10 秒単位で指定します。タイムアウトを指定しない場合は、既定値の **30** 秒が選択されます。
   ⓘ | **ヒント:** 「**Raw モード**」が選択されている場合、このフィールドは無視されます。
8. 「**モード**」を選択します。
   - **ブロードキャスト**
   - **マルチキャスト**
   - **両方**
9. 「**モード**」で「**マルチキャスト**」または「**両方**」を選択した場合は、「**マルチキャスト IP**」フィールドに、このプロトコルで使用する有効なマルチキャスト IP を指定します。
10. IP ヘルパー ポリシーによるパケット転送時に送信元 IP アドレスの変換を許可するには、「**送信元 IP の変換を許可する**」を選択します。このオプションは、既定では選択されています。
11. IP ヘルパー ポリシーによるパケットの転送時にキャッシュが作成されないようにするには、「**Raw モード**」を選択します。単方向の転送がサポートされています。このオプションは、既定では選択されていません。
    ⓘ | **補足:** 「**タイムアウト**」フィールドに設定されている時間は無視されます。
12. 「**保存**」を選択します。

ユーザ定義プロトコルの削除

ユーザ定義プロトコルを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. そのプロトコルの**削除**アイコンを選択します。

1 つまたは複数のユーザ定義リレー プロトコルを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 目的のプロトコルの（プロトコル名のそばにある）一番左のチェックボックスをオンにします。「**削除**」が使用可能になります。
3. 「**削除**」を選択します。

すべてのユーザ定義リレー プロトコルを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 「**リレー プロトコル**」テーブルのヘッダーにあるチェックボックスをオンにします。「**削除**」が使用可能になります。
3. 「**削除**」を選択します。

IP ヘルパー ポリシーの管理

IP ヘルパー ポリシーを使用すると、DHCP ブロードキャストと NetBIOS ブロードキャストをインターフェース間で転送できます。

重要: WAN インターフェースおよび NAT 向けに構成されたインターフェースについては、IP ヘルパーではサポートしていません。

トピック:

- IP ヘルパー ポリシーの追加
- IP ヘルパー ポリシーの編集
- IP ヘルパー ポリシーの削除
- TSR による IP ヘルパー キャッシュの表示

IP ヘルパー ポリシーの追加

追加できるポリシーは最大 256 個です。

IP ヘルパー ポリシーを追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー| ポリシー**」に移動します。
2. 「**+ 追加**」を選択します。「**IP ヘルパー ポリシーの追加**」ダイアログが表示されます。

3. このポリシーは既定で有効になっています。有効にせずにポリシーを設定するには、「**ポリシーを有効にする**」を無効にします。
4. 「**プロトコル**」メニューからプロトコルを選択します。既定は「**DHCP**」です。
5. 「**送信元**」で、送信元のインターフェースまたはゾーンを選択します。
6. 「**送信先**」で、以下のどちらかを選択します。
   - 送信先のアドレス グループまたはアドレス オブジェクト。
   - **ネットワークの作成**（新しいアドレス オブジェクトを作成する場合）。「**アドレス オブジェクトの追加**」ダイアログが表示されます。
7. 必要に応じて、「**コメント**」フィールドに任意のコメントを入力します。
8. 「**保存**」を選択します。

IP ヘルパー ポリシーの編集

IP ヘルパー ポリシーを編集するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 「**IP ヘルパー ポリシー**」テーブルで、該当するエントリの「**設定**」列にある**編集**アイコンを選択します。「**IP ヘルパー ポリシーの編集**」ダイアログが表示されます。

3. 設定項目は、「**IP ヘルパー ポリシーの追加**」ダイアログと同じです。このダイアログについては、「IP ヘルパー ポリシーの追加」を参照してください。

IP ヘルパー ポリシーの削除

ユーザ定義ポリシーを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. そのポリシーの「**ポリシー**」テーブルにある**削除**アイコンを選択します。

1 つまたは複数のユーザ定義ポリシーを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 目的のポリシーの（リレー プロトコルのそばにある）一番左のチェックボックスをオンにします。「**削除**」が使用可能になります。
3. 「**削除**」を選択します。

すべてのユーザ定義ポリシーを削除するには、以下の手順に従います。

1. 「**ネットワーク | システム > IP ヘルパー**」に移動します。
2. 「**ポリシー**」テーブルのヘッダーにあるチェックボックスをオンにします。「**削除**」が使用可能になります。
3. 「**削除**」を選択します。

表示される DHCP リレー リースのフィルタ

フィルタ機能を使用すると、「**アンチスプーフ キャッシュ**」テーブルおよび「**スプーフ検知リスト**」テーブルで特定の機器のみを表示できます。

テーブル表示をフィルタするには、以下の手順に従います。

1. 「**ネットワーク | システム > MAC-IP アンチスプーフ**」に移動します。
2. フィルタ対象のテーブルの下にある「**フィルタ**」フィールドで、機器の IP アドレス、インターフェース、MAC アドレス、ホスト名、名前のいずれかを指定します。このフィールドへの入力では、「」に示されている各演算子の適切な構文を使用する必要があります。フィルタ演算子の構文オプション.

フィルタ演算子の構文オプション

演算子	構文オプション
タイプを持つ値	• Ip=1.1.1.1 または ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
文字列	• X1 • 00:01 • Tst-mc • 1.1.
AND	Ip=1.1.1.1;iface=x1 Ip=1.1.1.0/24;iface=x1;just-string
または	Ip=1.1.1.1,2.2.2.2,3.3.3.0/24

演算子	構文オプション
	Iface=x1,x2,x3
否定	!ip=1.1.1.1;!just-string !iface=x1,x2
混在	Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05;just-string;!iface=x1,x2

TSR による IP ヘルパー キャッシュの表示

テクニカル サポート レポートでは、IP ヘルパー キャッシュ、現在のポリシーおよびプロトコルのすべてが次のように表示されます。

```
#IP_HELPER_START
IP ヘルパー
-----IP Helper Global Run-time Data-------
IP Helper is OFF
IP Helper - DHCP Relay is OFF
IP Helper - Netbios Relay is OFF
Total Number Of Fwded Packets :0
Total Number Of Dropped Packets :0
Total Number Of Passed Packets :0
Total Number Of Unknown Packets :0
Total Number Of record create failure :0
Total Number Of element create failure :0User-defined
-----IP Helper Applications -------
Name: DHCP
Port: 67, 68, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 3, index: 1, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: NetBIOS:
Port: 138, 137, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 4, index: 2, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: DNS
Port: 53, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 3, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: TIME
Port: 37, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 4, proto: 1,
Record Count: 0, Element Count: 0,
```

```
Fwded: 0, Dropped: 0, Passed: 0
Name: WOL
Port: 7, 9, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 5, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: mDNS
Port: 5353, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 6, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
----------GEN APP Relay Policy-----------
---------------------------------Record Table----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
-------------------------------------------------------------------------------
----------DHCP Relay Policy-----------
--------NETBIOS Relay Policy-----------
#IP_HELPER_END
```

10

動的ルーティング

トピック:

ルート通知

SonicWall セキュリティ装置は、RIPv1 または RIPv2 を使用して、その静的ルートおよび動的ルートをネットワーク上の他のルータに通知します。セキュリティ装置とリモート VPN ゲートウェイとの間で VPN トンネルの状況が変化した場合にも、RIPv2 で通知します。ご利用のルータの機能または設定に基づき、次のいずれかを選択します。

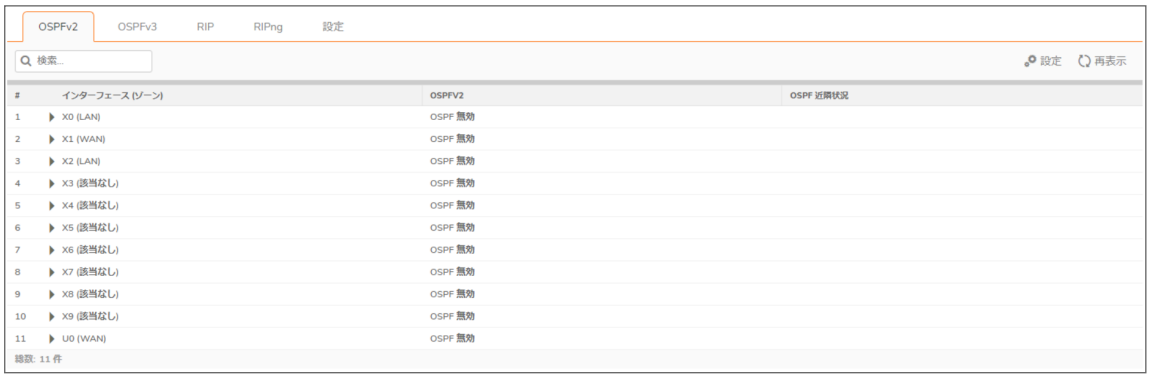
- RIPv1。プロトコルの初期バージョンであり、機能が少なく、マルチキャストではなくブロードキャストを使ってパケット送信を行います。
- RIPv2。プロトコルの後継バージョンであり、近隣ルータへのルーティング テーブルのマルチキャスト時のサブネット情報や、ルート学習のためのルート タグを含めます。RIPv2 パケットは下位互換性があり、マルチキャスト パケットのリッスンするオプションを提供する一部の RIPv1 実装でも受け付けることができます。「RIPv2 有効 (ブロードキャスト)」を選択すると、パケットをマルチキャストする代わりにブロードキャストします。これは RIPv1 ルータと RIPv2 ルータが混合する異機種ネットワークに適しています。

1. 「**ネットワーク | システム > 動的ルーティング | ルート通知**」は、「ルーティング モード」で「簡易 RIP 通知」が選択されている場合にのみ表示されます。

インターフェース (ゾーン)	ルート通知で設定されているインターフェース。インターフェースにゾーンが設定されていない場合、(**ゾーン**) 部分の表示は「(**該当なし**)」となります。
状況	「**有効**」または「**無効**」のどちらかです。
構成	**編集**アイコンが表示されています。

OSPFv2

「**ネットワーク | システム > 動的ルーティング > OSPFv2**」は、「**ルーティング モード**」で「**高度なルーティング モード**」が選択されている場合にのみ表示され、OSPFv2 の状況を示すとともにインターフェースに対する OSPFv2 の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示する、ページ右上のアイコン。次を参照してください。
インターフェース (ゾーン)	OSPFv2 で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、(ゾーン) 部分の表示は「(該当なし)」となります。
OSPFv2	OSPF がインターフェース上で有効になっているかどうかを示します。 • **OSPF 有効** • **OSPF 有効 (パッシブ)** • **OSPF 無効**
OSPF 近隣状況	動作中または停止中の近隣者があるかどうかを示す**状況**アイコンが表示されます。このアイコンを選択すると、インターフェースの近隣者に関する詳細を示す「**インターフェース OSPFv2 エリア近隣者**」ポップアップが表示されます。
構成	インターフェースの**編集**アイコンが表示されます。

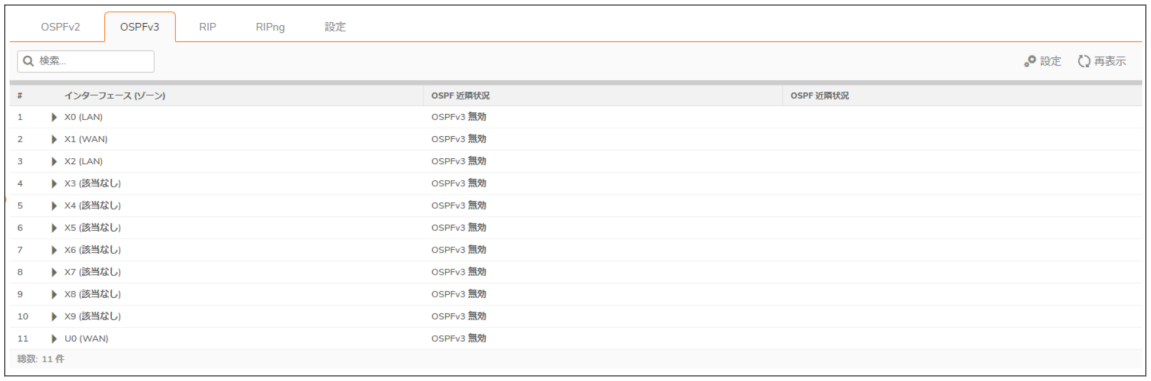
インターフェース OSPFv2 エリア近隣者

インターフェースの**状況**アイコンを選択すると、このポップアップが表示されます。

ルータ ID	近隣者のルータ ID。
現在の状況	確立された OSPFv2 近隣関係の状況。 • **Init（始動）** • **2-way（2 ウェイ）** • **ExStart（交換開始）** • **交換** • **Loading（ロード中）** • **完全**
優先順位	近隣者のルータの優先順位。
IP アドレス	近隣者のルータの IP アドレス。

OSPFv3

「**ネットワーク | システム > 動的ルーティング > OSPFv3**」は、「**ルーティング モード**」で「**高度なルーティング モード**」が選択されている場合にのみ表示され、OSPFv3 の状況を示すとともにインターフェースに対する OSPFv3 の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース（ゾーン）	OSPFv3 で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**（ゾーン）** 部分の表示は「**（該当なし）**」となります。
OSPFv3	OSPFv3 がインターフェース上で有効になっているかどうかを示します。 • **OSPFv3 有効** • **OSPFv3 有効（パッシブ）** • **OSPFv3 無効**
OSPFv3 の設定	インターフェースの**編集**アイコンが表示されます。
OSPFv3 近隣状況	動作中または停止中の近隣者があるかどうかを示す**状況**アイコンが表示されます。このアイコンを選択すると、インターフェースの近隣者に関する詳細を示す「**インターフェース OSPFv3 近隣者**」ポップアップが表示されます。「**ネットワーク	システム > 動的ルーティング > OSPFv3** > インターフェース OSPFv3 近隣者」を参照してください。

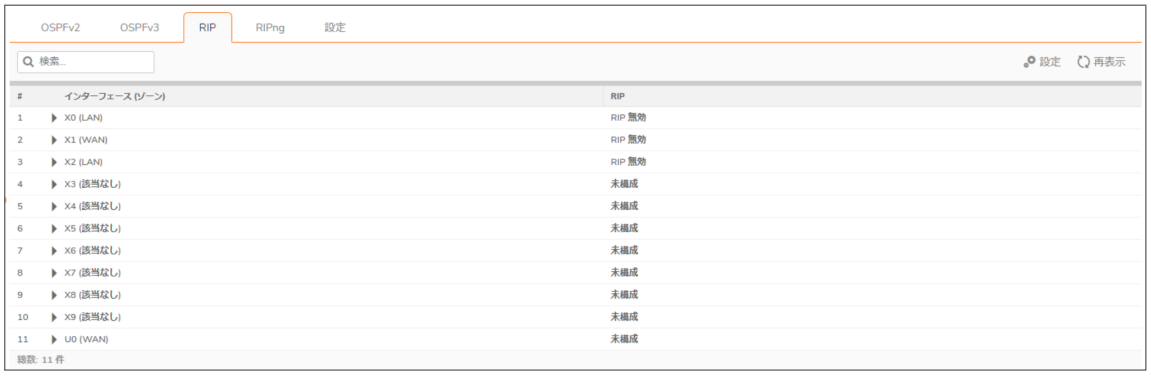
インターフェース OSPFv3 近隣者

インターフェースの **OSPF 近隣状況**アイコンを選択すると、このポップアップが表示されます。

ルータ ID	近隣者のルータ ID。
現在の状況	確立された OSPFv3 近隣関係の状況。 • **Init (始動)** • **2-way (2 ウェイ)** • **ExStart (交換開始)** • **交換** • **Loading (ロード中)** • **完全**
優先順位	近隣者のルータの優先順位。

RIP

「**ネットワーク | システム > 動的ルーティング > RIP**」は、「**ルーティング モード**」で「**高度なルーティング モード**」が選択されている場合にのみ表示され、RIP の状況を示すとともにインターフェースに対する RIP の設定を可能にします。

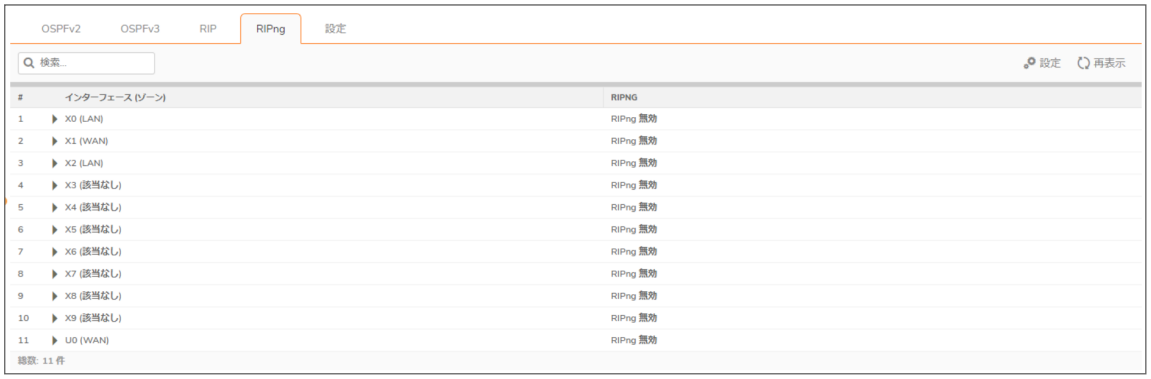


設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	RIP で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。

RIP	RIP がインターフェース上で有効になっているかどうかを示します。 • **RIP 有効** • **RIP 有効 (パッシブ)** • **RIP 無効**
RIP の設定	インターフェースの**編集**アイコンが表示されます。

RIPng

「**ネットワーク | システム > 動的ルーティング > RIPng**」は、「**ルーティング モード**」で「**高度なルーティング モード**」が選択されている場合にのみ表示され、RIPng の状況を示すとともにインターフェースに対する RIPng の設定を可能にします。



設定	デフォルト ルートに対するメトリックを設定するための「**設定**」ポップアップを表示するアイコン。
インターフェース (ゾーン)	RIPng で設定されているインターフェースとそのゾーン。インターフェースにゾーンが設定されていない場合、**(ゾーン)** 部分の表示は「**(該当なし)**」となります。
RIPng	RIPng がインターフェース上で有効になっているかどうかを示します。 • **RIPng 有効** • **RIPng 有効 (パッシブ)** • **RIPng 無効**
RIPng の設定	インターフェースの**編集**アイコンが表示されます。

設定

動的ルーティング設定を有効にするには、以下の手順に従います。

1. 「**ネットワーク | システム > 動的ルーティング | 設定**」に移動します。

2. 必要に応じて「**ルート クラス内でメトリックによるルートの優先付けをする**」を有効にします。
3. 高度なルーティング モードに切り替えるには、「**高度なルーティング モード**」を選択します。確認メッセージが表示されます。
4. BGP を有効にするには、「**BGP**」で「**有効 (CLI での設定)**」を選択します。既定は「**無効**」です。確認メッセージが表示されます。

11

DHCP サーバ

トピック:

DHCP サーバの設定

「**ネットワーク | システム > DHCP サーバ | DHCP サーバ設定 > IPv4/IPv6**」の IPv6 版と IPv4 版には、わずかな違いしかありません。手順には相違点があります。

IPV4 の DHCP サーバ設定

IPV6 の DHCP サーバ設定

装置には、IP アドレス、サブネット マスク、ゲートウェイ アドレス、および DNS サーバ アドレスをネットワーク クライアントに配布する DHCP (Dynamic Host Configuration Protocol) サーバが搭載されています。装置の DHCP サーバの設定は、「**ネットワーク | システム > DHCP サーバ | DHCP サーバ設定**」で行います。

ⓘ **重要:** 装置の DHCP サーバを使用することも、ネットワーク上の既存の DHCP サーバを使用することもできます。ネットワーク独自の DHCP サーバを使用する場合は、「**DHCP サーバを有効にする**」をオフにしてください。

ファイアウォールの DHCP サーバが割り当てることができるアドレス範囲と IP アドレスの数は、装置のモデル、オペレーティング システム、およびライセンスによって異なります。

トピック:

DHCP サーバの設定

SonicWall セキュリティ装置の DHCP サーバを使用するには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCP サーバ設定**」に移動します。
2. 使用する IP バージョン (IPv4 または IPv6) を選択します。

   IPV4

   IPV6

3. IP アドレス、サブネット マスク、ゲートウェイ アドレス、および DNS サーバ アドレスをネットワーク クライアントに配布するために、「**DHCPv4/6 サーバを有効にする**」を選択します。このオプションは、既定では選択されています。IPv4 の場合、「**詳細**」オプションとその他のサーバ設定オプションが使用可能になります。
4. DHCPv6 を設定する場合は、ステップ 7 に進みます。
5. 別の DHCP サーバが存在する場合に各ゾーンで自動 DHCP スコープ競合検出を有効にするには、「**競合の検出を有効にする**」を選択します。このオプションは、既定では選択されています。

現在、DHCP サーバは、この機能が有効な場合にサーバ側の競合検出を実施します。サーバが輪の競合検出の優位点は、DHCP クライアントがクライアント側の競合検出を実行しない場合でも競合を検出することにあります。しかしながら、ネットワーク上に多数の DHCP クライアントがある場合は、サーバ側の競合検出では、完全な IP アドレス割り当てを完了するために、より長い待ち時間を要することがあります。

ⓘ **補足:** 競合検出は、"リレーされる" サブネット スコープに属する IP アドレスに対しては実行されません。DHCP サーバはインターフェースに結びついているサブネット範囲に対してのみ、競合検出の ICMP 確認を実行します。

6. ネットワーク内の DHCP リースの現在の状況が定期的にフラッシュに書き込まれるようにするには、「**DHCP サーバ恒久割り当てを有効にする**」を選択します。再起動時に、システムはフラッシュに保存された IP リース回数に基づいて、以前の DHCP サーバ ネットワークの DHCP 割り当て情報を復元します。復元します。このオプションは、既定では選択されています。このオプションを選択すると、「**DHCP サーバ持続監視間隔**」オプションが使用可能になります。
    - ネットワークの変化を調査し、必要に応じてフラッシュに書き込む頻度を制御するには、「**DHCP サーバ持続監視間隔**」に時間間隔を分単位で入力します。既定値は **5** 分、最小値は 5 分、最大値は 1440 分 (24 時間) です。
7. **オプション オブジェクト**、**オプション グループ**、および**信頼されたエージェント**を設定するには、「**詳細**」を選択します。これらの機能を設定するための詳細な情報については、「*詳細オプションの設定*」を参照してください。
8. 「**適用**」を選択します。

トピック:

- DNS プロキシのための DHCP サーバの設定

DNS プロキシのための DHCP サーバの設定

インターフェースで DNS プロキシが有効になっている場合、機器はインターフェース IP を DNS サーバ アドレスとしてクライアントにプッシュする必要があるので、DHCP サーバを手動で設定し、「**DNS/WINS**」タブの DHCP サーバの設定でインターフェース アドレスを「DNS サーバ 1」のアドレスとして使用する必要があります。DHCP ページの「**インターフェースの事前設定**」チェックボックスを使用すると、この設定を簡単に行うことができます。選択したインターフェースで DNS プロキシが有効になっている場合、「**DNS/WINS**」ページに DNS サーバの IP が自動的に追加されます。

DHCP サーバ リース範囲の設定

DHCPV4 サーバ リース範囲

DHCPV6 サーバ リース スコープ

「**DHCP サーバ リース範囲**」テーブルには、現在設定されている DHCP の IP 範囲が表示されます。

DHCP サーバ リース範囲

種別	**動的**または**静的**
接頭辞	IPv6 のみ。
リース範囲	IP アドレスの範囲（例えば、172.16.31.2 — 172.16.31.254）。
インターフェース	IPv4 のみ。そのアドレス範囲が割り当てられるインターフェース。
詳細	**コメント** アイコンの上にマウス ポインタを置くと、リースに関する詳細情報がツール チップとして表示されます。
有効	DHCP 範囲を有効にするには、このチェックボックスをオンにします。範囲を無効にする場合は、チェックボックスをオフにします。
構成	テーブルの登録に対する**設定**アイコンと削除アイコンがあります。

現在の DHCP リース

トピック:

- 現在のIPv4 DHCP リース
- 現在のIPv6 DHCP リース

現在の IPv4 DHCP リース

「**現在の DHCP リース**」テーブルには、現在の DHCP リース情報が表示されます。各バインド エントリに表示される情報は以下のとおりです。

- **IP アドレス**
- **ホスト名**
- **リース存続期間**
- **MAC アドレス**
- **ベンダー**
- **種別**（**動的**、**動的 BOOTP**、または**静的 BOOTP**）
- **削除**

バインドを削除して DHCP サーバで IP アドレスを解放するには、以下の手順に従います。

1. エントリの横にある**削除**アイコンを選択します。例えば、ネットワークからホストが削除されていて、その IP アドレスを再利用する必要がある場合は、**削除**アイコンを使用します。
2. 「**適用**」を選択します。

現在のIPv6 DHCP リース

「現在の DHCP リース」テーブルには、現在の DHCP リース情報が表示されます。各バインド エントリに表示される情報は以下のとおりです。

- **IP アドレス**
- **リース存続期間**
- **IAID**
- **DUID**
- **種別**（**動的**、**動的 BOOTP**、または**静的 BOOTP**）
- **削除**

バインドを削除して DHCP サーバで IP アドレスを解放するには、以下の手順に従います。

1. エントリの横にある**削除**アイコンを選択します。例えば、ネットワークからホストが削除されていて、その IP アドレスを再利用する必要がある場合は、**削除**アイコンを使用します。
2. 「**適用**」を選択します。

DHCPv6 リレー

SonicOS では、DHCPv6 リレーがサポートされます。SonicOS の DHCPv6 リレーについては、「*DHCPv6 リレー*」を参照してください。

詳細オプションの設定

ⓘ **補足:** DHCP サーバのオプションの設定は、IPv4 と IPv6 のどちらでもほぼ同じです。相違点については、手順の中で示します。

トピック:

- DHCP オプション オブジェクトの設定
- DHCP オプション グループの設定
- 信頼された DHCP リレー エージェント アドレス グループの設定（IPv4 のみ）
- 信頼された DHCP リレー エージェントの有効化

各 DHCP オプションの説明は、「*RFC で定義された DHCP オプション番号*」の一覧表（RFC で割り当てられたオプション番号順）にまとめてあります。

DHCP オプション オブジェクトの設定

DHCP オプション オブジェクトを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCPv4/6 サーバ設定**」に移動します。
2. 「**詳細**」を選択します。「DHCP 詳細設定」ダイアログが表示されます。IPv4 と IPv6 のダイアログはわずかに異なります。「*IPv4 DHCP 詳細設定*」および「*IPv6 DHCP 詳細設定*」を参照してください。

IPV4 の「DHCP 詳細設定」

IPV6 の「DHCP 詳細設定」

3. 「**+ 追加**」を選択します。「**DHCP オプション オブジェクトの追加**」ダイアログが表示されます。

4. 「**オプション名**」フィールドにオプションの名前を入力します。
5. 「**オプション番号**」で、目的の DHCP オプションに対応するオプション番号を選択します。オプションの番号、名前、および説明の一覧については、「*RFC で定義された DHCP オプション番号*」を参照してください。

   ⓘ **補足:** 利用可能なオプションは、IPv4 または IPv6 のどちらのオプションを設定しているかによって異なります。

6. 次の場合:

   - 「**オプション番号**」で「2 (タイム オフセット)」を選択したときなど、該当するオプション種別が 1 つしかない場合は、「**オプション配列**」は淡色表示されます。ステップ 7 に進みます。

- 例えば、「**77 (ユーザ クラス情報)**」では、「**オプション種別**」が使用可能になり、このオプションで使用できるタイプとして「**IP アドレス**」、「**2 バイト データ**」、「**文字列**」、「**論理型**」などがリストされます。オプション種別を選択します。

7. オプションの値 (例えば、IP アドレスなど) を「**オプション値**」フィールドに入力します。「**オプション配列**」チェックボックスがオンの場合は、複数の値をセミコロン (;) で区切って入力することができます。
8. 「**OK**」を選択します。設定したオブジェクトが「**オプション オブジェクト**」テーブルに表示されます。

DHCP オプション グループの設定

DHCP オプション グループを設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCPv4/6 サーバ設定**」に移動します。
2. 「**詳細**」を選択します。「**DHCP 詳細設定**」ダイアログが表示されます。

   ⓘ **補足:** 利用可能なオプションは、IPv4 オプションまたは IPv6 オプションのどちらを設定するかによって異なります (「IPv6 DHCP 詳細設定」または「IPv4 DHCP 詳細設定」を参照)。

3. 「**オプション グループ**」を選択します。
4. 「**グループの追加**」をクリックします。「**DHCPv6 オプション グループの追加**」ダイアログが表示されます。
5. グループの名前を「**名前**」フィールドに入力します。
6. 「グループ内」に追加するオプション オブジェクトを左の列から選択して、**右矢印**を選択します。同時に複数のオプション オブジェクトを選択するには、Ctrl キーを押しながらオプション オブジェクトを選択します。
7. 「**OK**」を選択します。設定したグループが「**オプション グループ**」テーブルに表示されます。

信頼された DHCP リレー エージェント アドレス グループの設定 (IPv4 のみ)

「**既定の信頼されたリレー エージェント リスト**」アドレス グループを設定するには、最初に信頼できる各リレー エージェントに対してアドレス オブジェクトを設定した後、これらのアドレス オブジェクトを「**既定の信頼されたリレー エージェント リスト**」アドレス グループまたはカスタム アドレス グループに追加します。

アドレス オブジェクトとアドレス グループは「**オブジェクト | 一致オブジェクト > アドレス | アドレス オブジェクト**」で設定します。アドレス オブジェクトとアドレス グループを設定する方法については、『*SonicOS オブジェクト管理ガイド*』を参照してください。

信頼された DHCP リレー エージェントの有効化

「**DHCP 詳細設定**」ダイアログでは、「**既定の信頼されたリレー エージェント リスト**」アドレス グループを使用して「**信頼されたリレー エージェント リスト**」オプションを有効にするか、または既存のアドレス オブジェクトを使用して別のアドレス グループを作成できます。

ⓘ **補足:** サーバが VPN セントラル ゲートウェイを越えた DHCP で内部 DHCP サーバとして割り当てられている場合、VPN トンネルからの DHCP メッセージは常にバイパスされます。

「信頼されたリレー エージェント リスト」オプションを有効にして目的のアドレス グループを選択するには、次の手順を実行します。

1. 「**ネットワーク | システム > DHCP サーバ | DHCPv4 設定**」に移動します。
2. 「**詳細**」を選択します。「**DHCP 詳細設定**」ダイアログが表示されます。
3. 「**その他**」ビューを選択します。
4. 「**信頼された DHCP リレー エージェント リストを有効にする**」を選択します。このオプションは、既定では選択されていません。「**信頼されたリレー エージェント リスト**」が使用できるようになります。
5. 「**既定の信頼されたリレー エージェント リスト**」からアドレス グループを選択します。このオプションには、既存のすべてのアドレス グループと共に、「**アドレス オブジェクト グループの作成**」オプションが含まれます。
6. このオプションのカスタム アドレス グループを作成するには、「**アドレス オブジェクト グループの作成**」を選択します。「**アドレス オブジェクト グループの追加**」ダイアログが表示されます。アドレス グループを設定する方法については、『*SonicOS オブジェクト管理ガイド*』を参照してください。
7. 「**OK**」を選択し、選択したアドレス グループで「**信頼されたリレー エージェント リスト**」オプションを有効にします。

IPv4 DHCP サーバの動的範囲の設定

SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

IPv4 DHCP サーバの動的 IP アドレス範囲を設定するには、次の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCP サーバ リース範囲**」に移動します。
2. 「**+ 動的登録の追加**」を選択します。
    - 「**動的範囲の設定**」ダイアログが表示されます。「 DHCPサーバの動的範囲の追加

DHCPサーバの動的範囲の追加

動的範囲を追加するには、以下の手順に従います。

1. この範囲を有効にするには、「**一般**」ビューから「**この DHCP 範囲を有効にする**」を選択します。このオプションは、既定では選択されています。
2. 「**範囲開始**」、「**範囲終了**」、「**デフォルト ゲートウェイ**」、および「**サブネット マスク**」フィールドを設定するには:
   a. 特定のインターフェースで既定値を使用するには:
      1. ダイアログの下の方にある「**インターフェースの事前設定**」を選択します。選択されているオプションが使用可能になります。このオプションは、既定では選択されていません。
      2. インターフェースを選択します。設定される IP アドレスは、選択したインターフェースと同じプライベート サブネットの IP アドレスです。

      ⓘ **重要:**「**インターフェースの事前設定**」からインターフェースを選択するには、対象のインターフェースをあらかじめ完全に設定しておく必要があります。
      - ゾーン タイプの LAN、WLAN、または DMZ。
      - VLAN サブインターフェース。
      - ステップ 3 に進みます。

   b. 手動:
      1. 独自のIP アドレス範囲を入力します。
      2. 「リース期間 (分)」フィールドに、別の IP アドレスが発行されるまで範囲によって IP アドレスがリースされる時間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は 1440 (24 時間) です。
      3. ゲートウェイの IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。
      4. ゲートウェイのサブネット マスクを「**サブネット マスク**」フィールドに入力します。
3. 必要に応じて、「**コメント**」フィールドにコメントを入力します。

4. ネットワークに BOOTP クライアントがある場合、「**BootP クライアントによる DHCP アドレス範囲の利用を許可する**」を選択します。このオプションは、既定では選択されていません。

   BOOTP は Bootstrap Protocol の略であり、ディスクを持たないワークステーションが自分の IP アドレス、他の TCP/IP 設定情報、起動イメージ ファイルを BOOTP サーバから取得することを実現する TCP/IP プロトコルおよびサービスです。
5. 「**DNS/WINS**」を選択して、DHCP サーバ機能の設定を続けます。

DNS/WINS

DNS/WINS サーバを設定するには、以下の手順に従います。

1. DNS サーバのドメイン名がある場合は、「**ドメイン名**」フィールドに入力します。
2. 次のどちらかを行います。
   - 「**WAN ゾーンと同じ DNS サーバ設定にする**」を選択し、ステップ 4 へ進みます。
   - 「**手動で指定する**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。
3. 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。
4. ネットワーク上で WINS が実行されている場合は、「**WINS サーバ 1**」フィールドに WINS サーバの IP アドレスを入力します。さらに別の WINS サーバも追加できます。
5. 「**詳細**」を選択します。「**詳細**」オプションでは、Cisco コール マネージャ情報をネットワーク上の VoIP クライアントに送信するように、DHCP サーバを設定できます。

詳細

詳細設定を行うには、以下の手順に従います。

1. 「**VoIP コール マネージャ**」で、「**コール マネージャ 1**」フィールドに VoIP コール マネージャの IP アドレスまたは FDQN を入力します。さらに 2 つの VoIP コール マネージャ アドレスを追加できます。
2. 「**ネットワーク起動設定**」で、「**次のサーバ**」フィールドに、起動プロセスの次のステージの間に PXEクライアントが使用する PXE 起動サーバ（TFTP サーバ）の IP アドレスを入力します。

   ⓘ **重要:**「**ネットワーク起動設定**」の下のフィールドは Pre－boot Execution Environment（PXE）で使われるものであり、クライアントはネットワーク インターフェースから取得したファイルを使用して起動します。PXE クライアントは、PXE 起動サーバの IP アドレスと名前および起動ファイル名を、DHCPサーバから取得します。
   これらのオプションを使用するときは、「**DHCP 汎用オプション**」の「**PXE**」を選択します。
3. 「**起動ファイル**」フィールドに、PXE クライアントが PXE 起動サーバから TFTP 経由で取得できる起動ファイルの名前を入力します。
4. 「**サーバ名**」フィールドに、PXE 起動サーバ（TFTP サーバ）の DNS ホスト名を入力します。
5. **DHCP 汎用オプション**の設定については、「*DHCP リース範囲の DHCP 汎用オプションの設定*」を参照してください。
6. 「**OK**」を選択します。
7. 「**適用**」を選択してファイアウォールに設定を適用します。

SonicWall セキュリティ装置の VoIP サポート機能の詳細については、「*VoIP*」を参照してください。

IPv6 DHCP サーバの動的範囲の設定

SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

IPv6 DHCP サーバの動的 IP アドレス範囲を設定するには、次の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCPv6 サーバ リース範囲**」に移動します。
2. 「**+ 動的登録の追加**」を選択します。
   - 「**DHCPv6 動的スコープの追加**」ダイアログが表示されます。「*DHCPv6 動的スコープの追加*」に進んでください。
   - IPv4 の場合、「**動的範囲構成**」ダイアログが表示されます。「*動的範囲構成*」に進んでください。

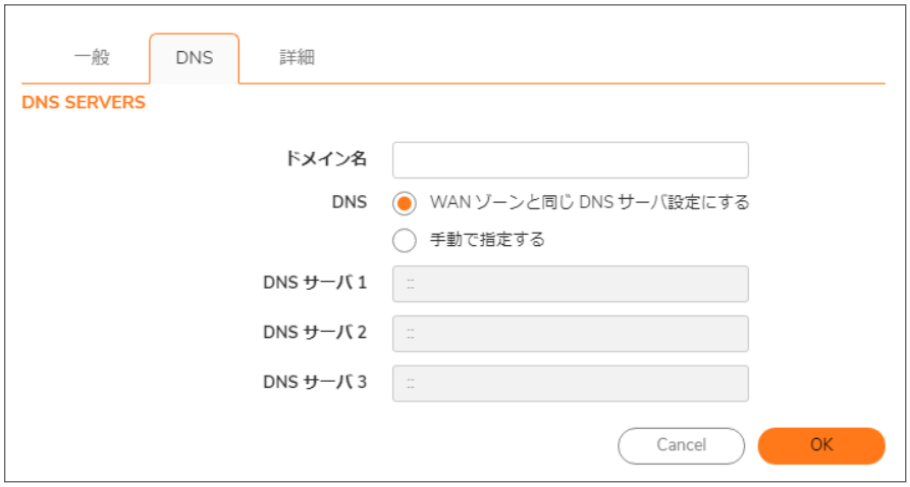
DHCPv6 動的スコープの追加

動的範囲を追加するには、以下の手順に従います。

1. この範囲を有効にするには、「**この DHCP 範囲を有効にする**」を選択します。このオプションは、既定では選択されています。
2. 「**名前**」フィールドに範囲の名前を入力します。
3. 「**接頭辞**」フィールドに、この範囲で IPv6 アドレスの配布に使用する接頭辞を入力します。
4. 「**範囲開始**」フィールドと「**範囲終了**」フィールドに、範囲の開始アドレスと終了アドレスを入力します。両方のアドレスが接頭辞の範囲内である必要があります。

5. 「**有効存続期間**」フィールドに、範囲によってリースされる IPv6 アドレスの有効存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **2160** です。
6. 「**優先存続期間**」フィールドに、範囲によってリースされる IPv6 アドレスの優先存続期間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** です。
7. 必要に応じて、「**コメント**」フィールドにコメントを入力します。
8. 「**DNS**」を選択します。

DNS



DNS サーバを追加するには、以下の手順に従います。

1. 「**ドメイン名**」フィールドにドメイン名を入力します。
2. 次のどちらかを行います。
   - 「**WAN ゾーンと同じ DNS サーバ設定にする**」を選択し、ステップ 4 へ進みます。
   - 「**手動で指定する**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。
3. 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。
4. 「**詳細**」を選択します。

詳細

汎用的な DHCP オプションを設定するには、以下の手順に従います。

1. 「DHCPv6 汎用オプション」で、DHCP オプション オブジェクトまたはグループを選択します。既定は「**なし**」です。新しい DHCPv6 オプションまたはグループを設定するには、「DHCP オプション オブジェクトの設定」または「DHCP オプション グループの設定」を参照してください。
2. DHCPv6 クライアントからのメッセージに含まれるオプション要求オプションに関係なく、この範囲に設定されているすべての DHCPv6 オプションを送信するには、「**DHCPv6 オプションを常に送信する**」を有効にします。このオプションは、既定では選択されていません。
3. 「**OK**」を選択します。

IPv4 DHCP 静的登録の設定

静的登録は、永続的な IP 設定を要求するサーバに割り当てられる IP アドレスです。SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

静的登録を設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCP サーバ リース範囲**」テーブルに移動して、「**+ 静的登録の追加**」を選択します。

   「**静的範囲構成**」ダイアログが表示されます。「*静的範囲構成*」に進んでください。

DHCPv4 静的登録の追加

この範囲を有効にするには、以下の手順に従います。

1. 「**この DHCP 範囲を有効にする**」を選択します。このオプションは、既定では選択されています。
2. 「**登録名**」フィールドに、静的登録の名前を入力します。

3. 「**静的 IP アドレス**」フィールドに、機器の IP アドレスを入力します。
4. 「**MAC アドレス**」フィールドに、機器のイーサネット (MAC) アドレスを入力します。
5. 「**リース期間**」、「**デフォルト ゲートウェイ**」、および「**サブネット マスク**」の各フィールドに特定のインターフェースの既定値を設定するには、ダイアログの下の方にある「**インターフェースの事前設定**」をオンにします。ドロップダウン メニューが使用可能になります。このオプションは、既定では選択されていません。

    a. ドロップダウン メニューで、インターフェースを選択します。設定される IP アドレスは、選択したインターフェースと同じプライベート サブネットの IP アドレスです。

    ⓘ **重要**:「インターフェース」メニューからインターフェースを選択するには、対象のインターフェースをあらかじめ完全に設定しておく必要があります。選択できるのは、LAN、WLAN、DMZ のいずれかのゾーン タイプ、または VLAN サブインターフェースのみです。

6. 「**リース期間 (分)**」フィールドに、別の IP アドレスが発行されるまで範囲によって IP アドレスがリースされる時間を分単位で入力します。最小値は 0、最大値は 71582789、既定値は **1440** (24 時間) です。
7. 設定されているゲートウェイ アドレスを使用するか、ゲートウェイの IP アドレスを「**デフォルト ゲートウェイ**」フィールドに入力します。
8. 設定されているサブネット マスクを使用するか、ゲートウェイのサブネット マスクを「**サブネット マスク**」フィールドに入力します。
9. 必要に応じて、「**コメント**」フィールドにコメントを入力します。
10. DNS/WINS 設定と詳細設定の設定方法については、「*DNS/WINS*」および「*詳細*」を参照してください。
11. 「**OK**」を選択してファイアウォールに設定を追加します。
12. 「**適用**」を選択してファイアウォールに設定を適用します。

SonicWall セキュリティ装置の VoIP サポート機能の詳細については、「*VoIP*」を参照してください。

DNS/WINS

DNS/WINS サーバを設定するには、以下の手順に従います。

1. DNS サーバのドメイン名がある場合は、「**ドメイン名**」フィールドに入力します。
2. 次のどちらかを行います。
   - 「**WAN ゾーンと同じ DNS サーバ設定にする**」を選択し、ステップ 4 へ進みます。
   - 「**手動で指定する**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。
3. 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。
4. ネットワーク上で WINS が実行されている場合は、「**WINS サーバ 1**」フィールドに WINS サーバの IP アドレスを入力します。さらに別の WINS サーバも追加できます。
5. 「**詳細**」を選択します。「**詳細**」オプションでは、Cisco コール マネージャ情報をネットワーク上の VoIP クライアントに送信するように、DHCP サーバを設定できます。

詳細

詳細設定を行うには、以下の手順に従います。

1. 「**VoIP コール マネージャ**」で、「**コール マネージャ 1**」フィールドに VoIP コール マネージャの IP アドレスまたは FDQN を入力します。さらに 2 つの VoIP コール マネージャ アドレスを追加できます。
2. 「**ネットワーク起動設定**」で、「**次のサーバ**」フィールドに、起動プロセスの次のステージの間に PXEクライアントが使用する PXE 起動サーバ（TFTP サーバ）の IP アドレスを入力します。

   重要：「**ネットワーク起動設定**」の下のフィールドは Pre－boot Execution Environment（PXE）で使われるものであり、クライアントはネットワーク インターフェースから取得したファイルを使用して起動します。PXE クライアントは、PXE 起動サーバの IP アドレスと名前および起動ファイル名を、DHCPサーバから取得します。

これらのオプションを使用するときは、「**DHCP 汎用オプション**」の「**PXE**」を選択します。

3. 「**起動ファイル**」フィールドに、PXE クライアントが PXE 起動サーバから TFTP 経由で取得できる起動ファイルの名前を入力します。
4. 「**サーバ名**」フィールドに、PXE 起動サーバ（TFTP サーバ）の DNS ホスト名を入力します。
5. **DHCP 汎用オプション**の設定については、「*DHCP リース範囲の DHCP 汎用オプションの設定*」を参照してください。
6. 「**OK**」を選択します。
7. 「**適用**」を選択してファイアウォールに設定を適用します。

SonicWall セキュリティ装置の VoIP サポート機能の詳細については、「*VoIP*」を参照してください。

IPv6 DHCP 静的範囲の設定

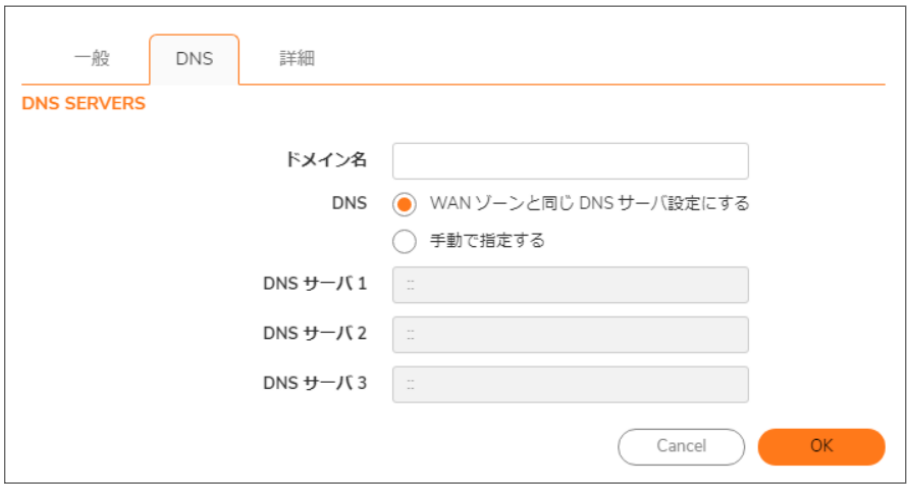
静的範囲は、永続的な IP 設定を要求するサーバに割り当てられる IP アドレスです。SonicOS ではインターフェースごとに複数の DHCP スコープを設定できるので、DHCP スコープを設定するときにサブネット範囲がインターフェースに接続されている必要はありません。

静的範囲を設定するには、以下の手順に従います。

1. 「**ネットワーク | システム > DHCP サーバ | DHCPv6 サーバ リース範囲**」テーブルに移動して、「**+ 静的登録の追加**」を選択します。

   「**DHCPv6 静的スコープの追加**」ダイアログが表示されます。「*静的スコープ設定*」に進んでください。

DNS



DNS サーバを追加するには、以下の手順に従います。

1. 「**ドメイン名**」フィールドにドメイン名を入力します。
2. 次のどちらかを行います。
   - 「**WAN ゾーンと同じ DNS サーバ設定にする**」を選択し、ステップ 4 へ進みます。
   - 「**手動で指定する**」を選択します。「**DNS サーバ 1/2/3**」フィールドが使用可能になります。

3. 「**DNS サーバ 1/2/3**」フィールドに、それぞれの DNS サーバの IP アドレスを入力します。
4. 「**詳細**」を選択します。

詳細

汎用的な DHCP オプションを設定するには、以下の手順に従います。

1. 「DHCPv6 汎用オプション」で、DHCP オプション オブジェクトまたはグループを選択します。既定は「**なし**」です。新しい DHCPv6 オプションまたはグループを設定するには、「DHCP オプション オブジェクトの設定」または「DHCP オプション グループの設定」を参照してください。
2. DHCPv6 クライアントからのメッセージに含まれるオプション要求オプションに関係なく、この範囲に設定されているすべての DHCPv6 オプションを送信するには、「**DHCPv6 オプションを常に送信する**」を有効にします。このオプションは、既定では選択されていません。
3. 「**OK**」を選択します。

DHCP リース範囲の DHCP 汎用オプションの設定

ここでは、リース範囲の DHCP 汎用オプションの設定作業について説明します。

ⓘ **補足:** DHCP リース範囲の汎用オプションを設定するには、あらかじめ静的または動的な DHCP サーバ リース範囲を作成しておく必要があります。

各 DHCP オプションの説明は、「*RFC で定義された DHCP オプション番号*」の一覧表 (RFC で割り当てられたオプション番号順) にまとめてあります。

DHCP サーバ リース範囲の DHCP 汎用オプションを設定するには、以下の手順を実行します。

1. 次の場合:
    a. 既存の DHCP リース範囲に変更を加える場合:
        1. 「**ネットワーク | システム > DHCP サーバ**」の「DHCP サーバ リース範囲」テーブルを表示し、変更を加えるリース範囲のエントリを確認します。
        2. **設定**アイコンを選択します。
        3. 表示されるダイアログで「**詳細**」を選択します。
    b. 新しい DHCP リース範囲を作成する場合:
        1. 「**一般**」タブと「**DNS/WINS**」タブでオプションを設定してから「**詳細**」ビューを選択します (「DHCP サーバの動的スコープの設定」または「静的 DHCP 登録の設定」を参照してください)。

2. 「**DHCP 汎用オプション グループ**」ドロップダウン メニューで、DHCP オプションまたはオプション グループを選択します。

   「**ネットワーク起動設定**」のフィールドを PXE 用に設定する場合は、ここで「**PXE**」を選択します。
3. この DHCP サーバ リース範囲の DHCP オプションを常に使用する場合は、「**汎用オプションを常に送信**」チェックボックスをオンにします。
4. 「**OK**」を選択します。

RFC で定義された DHCP オプション番号

オプション番号	IPv6 √	名前	説明
2		タイムオフセット	協定世界時からのオフセット時間
3		ルータ	N/4 ルータのアドレス
4		タイムサーバ	N/4 タイム サーバのアドレス
5		ネームサーバ	N/4 IEN-116 ネーム サーバのアドレス
6		DNS サーバ	N/4 DNS サーバのアドレス
7		ログサーバ	N/4 ログ サーバのアドレス
8		Cookie サーバ	N/4 Cookie サーバのアドレス
9		LPR サーバ	N/4 プリンタ サーバのアドレス
10		Impress サーバ	N/4 Imagen Impress サーバのアドレス
11		RLP サーバ	N/4 リソース ロケーション サーバのアドレス
12	√	ホスト名	ホスト名の文字列 ((サーバ ユニキャスト) など)
13		ブートファイルサイズ	ブート ファイルのサイズ (512 バイト ブロックの数)
14		メリットダンプファイル	クライアントのコア イメージがダンプされるファイルの名前
15		ドメイン名	クライアントの DNS ドメイン名
16		Swap サーバ	スワップ サーバのアドレス
17		ルートパス	ルート ディスクのパス名
18		拡張ファイル	追加的な BOOTP 情報が含まれているファイルのパス名
19		IPレイヤ転送	IP 転送の有効化または無効化
20		ソースルーティング有効	ソースルーティング有効
21	√	ポリシー フィルタ (IPv4) SIP サーバ ドメイン名リスト (IPv6)	ルーティングに対するポリシー フィルタ (IPv4) SIP サーバ ドメイン名のリストを有効にする (IPv6)
22	√	最大 DG 再編成サイズ (IPv4) SIP サーバ IPv6 アドレス リスト (IPv6)	再編成するデータグラムの最大サイズ (IPv4) SIP サーバ IPv6 アドレスのリストを有効に

オプション番号	IPv6 √	名前	説明
			する (IPv6)
23	√	既定の IP TTL (IPv4) DNS 再帰名前サーバ (IPv6)	既定の IP 存続期間 (IPv4) DNS 再帰名前サーバのリストを有効にする (IPv6)
24	√	パスMTU 寿命タイムアウト (IPv4) ドメイン検索リスト (IPv6)	パスMTU 寿命タイムアウト (IPv4) 検索用ドメイン名のリストを有効にする (IPv6)
25		MTU 停滞	パス MTU 検出の実行時に使用する MTU サイズのテーブル
26		インタフェース MTUサイズ	インターフェース MTU サイズ
27	√	すべてのサブネットはローカル (IPv4) ネットワーク情報サービス (NIS) サーバ (IPv6)	すべてのサブネットはローカル (IPv4) ネットワーク情報サービス (NIS) サーバのリストを有効にする (IPv6)
28	√	ブロードキャスト アドレス (IPv4) ネットワーク情報サービス V2 (NIS+) サーバ (IPv6)	ブロードキャスト アドレス (IPv4) ネットワーク情報サービス V2 (NIS+) サーバのリストを有効にする (IPv6)
29	√	マスク検出の実行 (IPv4) ネットワーク情報サービス (NIS) ドメイン名 (IPv6)	マスク検出の実行 (IPv4) ネットワーク情報サービス (NIS) ドメイン名のリストを有効にする (IPv6)
30	√	マスクを他者に提供 (IPv4) ネットワーク情報サービス V2 (NIS+) ドメイン名 (IPv6)	マスクを他者に提供 (IPv4) ネットワーク情報サービス V2 (NIS+) ドメイン名のリストを有効にする (IPv6)
31	√	ルータ検出の実行 (IPv4) シンプル ネットワーク タイム プロトコル (SNTP) サーバ (IPv6)	ルータ検出の実行 (IPv4) シンプル ネットワーク タイム プロトコル (SNTP) サーバのリストを有効にする (IPv6)
32	√	ルータ要請アドレス (IPv4) 情報更新時間 (IPv6)	ルータ要請アドレス (IPv4) 情報更新時間 (IPv6)
33		静的ルーティング テーブル	静的ルーティング テーブル
34		Trailer カプセル化	トレーラの使用を試みるか否かを指定
35		ARP キャッシュ タイムアウト	ARP キャッシュのタイムアウト時間
36		イーサネット カプセル化	イーサネットのカプセル化を使用するか否かを指定
37		既定のTCP持続時間	既定の TCP 存続期間
38		TCP キープアライブ間隔	TCP キープアライブ メッセージの送信間隔
39		TCP キープアライブガーベイジ	TCP キープアライブ メッセージとともに互換性のための無意味なバイトを送信するか否かを指定
40		NIS ドメイン名	NIS ドメイン名
41		NIS サーバアドレス	NIS サーバアドレス
42		NTP サーバアドレス	NTP サーバアドレス
43		ベンダー固有情報	ベンダー固有情報

オプション番号	IPv6 √	名前	説明
44		NetBIOS ネームサーバ	NetBIOS ネーム サーバのアドレス
45		NetBIOS データグラム ディストリビューション	NetBIOS データグラム配信サーバのアドレス
46		NetBIOS ノード種別	NetBIOS ノードの種類
47		NetBIOS スコープ	NetBIOS スコープ
48		X Window フォントサーバ	X ウィンドウ フォント サーバのアドレス
49		X Window ディスプレイマネージャ	X ウィンドウ表示マネージャが実行されているシステムのアドレス
50		要求された IP アドレス	要求された IP アドレス
51		IP Address Lease Time	IP アドレスのリース期間
52		Option Overload	“sname”または“file”フィールドをオプション用に使用していることを示す
53		DHCP Message Type	DHCP メッセージの種類
54		DHCP サーバ証明	DHCP サーバの識別情報
55		Parameter Request List	要求するパラメータのリスト
56		メッセージ	DHCP エラー メッセージ
57		DHCP Maximum Message Size	DHCP メッセージの最大サイズ
58		Renew Time Value	DHCP リースの再取得を要求するまでの時間 (T1)
59		Rebinding Time Value	DHCP 再割り当てを要求するまでの時間 (T2)
60		クラス識別子	クラス識別子
61		クライアント識別子	クライアント識別子
62		Netware/IP ドメイン名	Netware/IP ドメイン名
63		Netware/IP サブオプション	Netware/IP サブ オプション
64		NIS+ V3 クライアントドメイン名	NIS+ V3 クライアントのドメイン名
65		NIS+ V3 サーバアドレス	NIS+ V3 サーバのアドレス
66		TFTP サーバ名	TFTP サーバ名
67		ブート ファイル名	ブート ファイル名
68		ホームエージェントアドレス	モバイル IP ホーム エージェントのアドレス
69		Simple Mail サーバアドレス	Simple Mail Transfer Protocol (SMTP) サーバのアドレス
70		Post Office サーバアドレス	Post Office Protocol (POP3) サーバのアドレス
71		Network News サーバアドレス	Network News Transfer Protocol (NNTP) サーバのアドレス
72		WWW サーバアドレス	WWW サーバのアドレス
73		Finger サーバアドレス	フィンガー サーバのアドレス

オプション番号	IPv6 √	名前	説明
74		Chat サーバアドレス	Internet Relay Chat (IRC) サーバのアドレス
75		StreetTalk サーバアドレス	StreetTalk サーバのアドレス
76		StreetTalk Directory Assistance アドレス	StreetTalk Directory Assistance (STDA) サーバのアドレス
77		ユーザ クラス情報	ユーザ クラス情報
78		SLP ディレクトリエージェント	Service Location Protocol (SLP) ディレクトリエージェントのアドレス
79		SLP サービススコープ	Service Location Protocol (SLP) エージェントのスコープ
80		急速コミット	急速コミットの使用
81		FQDN、完全修飾ドメイン名	完全修飾ドメイン名
82		リレー エージェント情報	リレー エージェント情報
83		インターネット ストレージネームサービス	Internet Storage Name Service (iSNS) サーバのアドレス
84			該当なし
85		Novell ディレクトリ サービス	Novell Directory Services (NDS) サーバのアドレス
86		Novell ディレクトリ サーバツリー名	Novell Directory Services (NDS) サーバ ツリー名
87		Novell ディレクトリ サーバ コンテキスト	Novell Directory Services (NDS) サーバ コンテキスト
88		BCMCS コントローラドメイン名リスト	Broadcast/Multicast Services (BCMCS) コントローラのドメイン名リスト
89		BCMCS コントローラ IPv4 アドレスリスト	BCMCS コントローラの IPv4 アドレス リスト
90		認証	認証
91 ～ 92			該当なし
93		クライアントシステム	クライアントのシステム手法の種類
94		クライアントネットワーク装置インタフェース	クライアントのネットワーク機器インターフェースの種類
95		LDAP 利用	Lightweight Directory Access Protocol (LDAP) の使用
96			該当なし
97		UUID/GUID ベースのクライアント識別子	UUID/GUID に基づくクライアント識別子
98		オープン グループのユーザ認証	オープン グループのユーザ認証サービスの URL
99 ～ 108			該当なし
109		自律システム番号	自律システム番号
110 ～ 111			該当なし

オプション番号	IPv6 √	名前	説明
112		NetInfo Parent サーバアドレス	NetInfo 親サーバのアドレス
113		NetInfo Parent サーバタグ	NetInfo 親サーバのタグ
114		URL:	URL
115			該当なし
116		自動構成	DHCP 自動設定
117		ネーム サービス検索	ネーム サービス検索
118		サブネット コレクション	サブネットの選択
119		DNS ドメイン検索リスト	DNS ドメイン検索リスト
120		SIP サーバ DHCP オプション	Session Initiation Protocol (SIP) サーバのドメイン名またはアドレス
121		クラス静的ルートオプション	クラスレス静的ルート オプション
122		CCC, CableLabs クライアント構成	CableLabs クライアントの設定オプション
123		GGeoConf	地理的位置設定情報
124		Vendor-Identifying ベンダークラス	ベンダー識別のためのベンダー種別情報
125		Vendor Identifying ベンダー固有	ベンダー識別のためのベンダー固有情報
126 ～ 127			該当なし
128		TFTP サーバ IPアドレス	IP 電話のソフトウェアを読み込むための TFTP サーバの IP アドレス
129		コールサーバ IPアドレス	コールサーバの IP アドレス
130		差別文字列	ベンダーを識別するための判別文字列
131		リモート統計サーバIPアドレス	リモート統計サーバの IP アドレス
132		802.1Q VLAN ID	IEEE 802.1Q の VLAN ID
133		802.1Q L2 優先順位	IEEE 802.1Q の第 2 層優先順位
134		Diffserv コードポイント	VoIP シグナルとメディア ストリームのための Diffserv コード ポイント
135		電話アプリケーションのHTTPプロキシ	電話固有アプリケーション用の HTTP プロキシ
136 ～ 149			該当なし
150		TFTP サーバ アドレス、イーサブート、GRUB 構成	TFTP サーバ アドレス、イーサブート、GRUB 構成
151 ～ 174			該当なし
175		イーサブート	イーサブート
176		IP 電話	IP 電話
177		イーサブート、PacketCable および CableHome	イーサブート、PacketCable および CableHome
178 ～ 207			該当なし
208		`pxelinux.magic` (文字列) = `241.0.116.126`	`pxelinux.magic` (文字列) = `241.0.116.126`

オプション番号	IPv6 √	名前	説明
209		pxelinux.configfile（テキスト）	pxelinux.configfile（テキスト）
210		pxelinux.pathprefix（テキスト）	pxelinux.pathprefix（テキスト）
211		pxelinux.reboottime	pxelinux.reboottime
212 ～ 219			該当なし
220		サブネット割り当て	サブネットの割り当て
221		仮想サブネット割り当て	仮想サブネットの選択
222 ～ 223			該当なし
224 ～ 254		プライベート利用	プライベート利用

DHCP と IPv6

SonicOS の IPv6 実装の詳細については、「*IPv6*」を参照してください。

12

マルチキャスト

IP マルチキャストは、1 つのインターネット プロトコル (IP) パケットを同時に複数のホストに送信する手法です。マルチキャストは、インターネット トラフィックで急速に大きな位置を占めつつあるマルチメディア プレゼンテーションおよびビデオ会議に適しています。例えば、1 つのホストからオーディオ ストリームとビデオ ストリームが送信され、そのストリームを 10 個のホストで受信するとします。マルチキャストの場合、送信側ホストは特定のマルチキャスト アドレスを使って 1 つの IP パケットを送信します。受信側の 10 個のホストでは、そのアドレス宛のパケットをリッスンして受信するように設定するだけで済みます。マルチキャストは、コネクションレス モードで動作するポイント ツー マルチポイント IP 通信メカニズムです。ホストでは、ラジオのように“チューニング”することでマルチキャスト送信ストリームを受信します。

「**ネットワーク | システム > マルチキャスト**」ページで、ファイアウォール上のマルチキャスト トラフィックを管理できます。

- **マルチキャストを有効にする** — マルチキャスト トラフィックをサポートするには、このオプションを選択します。このオプションは、既定では選択されていません。
- **マルチキャスト データ転送のために IGMP メンバーシップ レポートを要求する** — このオプションを選択すると、IGMP を使用してマルチキャスト グループ アドレスに追加されたインターフェースにのみマルチキャスト データを転送するように限定することで、パフォーマンスを向上します。このオプションは、マルチキャストが有効になっている場合にのみ使用できます。このオプションは、既定では選択されています。

- **マルチキャスト状況テーブル登録タイムアウト(分)** – マルチキャスト テーブル内の登録の有効期間(分)を入力します。この期間が経過すると、テーブルを作り直す必要があります。このフィールドの既定値は **5** です。このフィールドの値の範囲は 5～60(分)です。以下のような場合、既定のタイムアウト値を変更してください。
  - メンバーシップ問い合わせまたはメンバーシップ レポートがネットワーク上で失われている可能性がある。
  - ネットワーク上の IGMP トラフィックを減らしたいが、現在多数のマルチキャスト グループまたはマルチキャスト クライアントがある。これは、トラフィックをルーティングするルータがない状況の場合です。
  - IGMP ルータとタイミングを同期する必要がある。

トピック:

- マルチキャスト ポリシー
- SNMP 状況
- マルチキャストの有効化

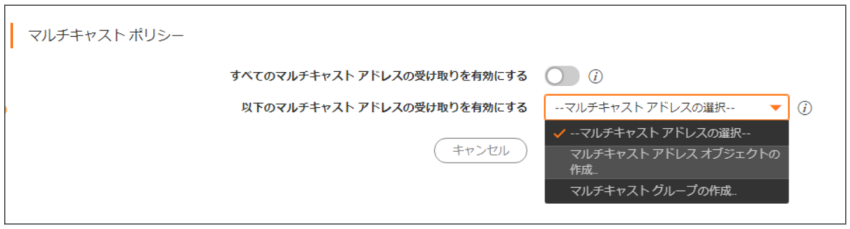
マルチキャスト ポリシー

ⓘ | **ヒント:** これらのオプションを使用するには、マルチキャストを有効にする必要があります。

- 「**すべてのマルチキャスト アドレスの受け取りを有効にする**」 – このラジオ ボタンは既定で無効になっています。このラジオ ボタンを選択すると、すべての(クラス D)マルチキャスト アドレスが受信されます。

  ⓘ | **補足:** すべてのマルチキャスト アドレスを受信した場合、ネットワークのパフォーマンスが低下する可能性があります。

- 「**以下のマルチキャスト アドレスの受け取りを有効にする**」– 既存のマルチキャスト オブジェクト/グループを選択します。また、新しいマルチキャスト オブジェクトまたは新しいマルチキャスト グループを作成して、ドロップダウン メニューに表示させることもできます。ドロップダウン メニューで、「**マルチキャスト アドレス オブジェクトの作成**」または「**マルチキャスト グループの作成**」を選択します。



  ⓘ | **補足:** MULTICAST ゾーンに関連付けられているアドレス オブジェクトおよびアドレス グループのみ選択できます。MULTICAST ゾーンに関連付けられるのは、224.0.0.1 ～ 239.255.255.255 の範囲のアドレスのみです。

  ⓘ | **補足:** 指定できるマルチキャスト アドレスは最大 200 個です。

トピック:

- マルチキャスト アドレス オブジェクトの作成

マルチキャスト アドレス オブジェクトの作成

マルチキャスト アドレス オブジェクトを作成するには、以下の手順に従います。

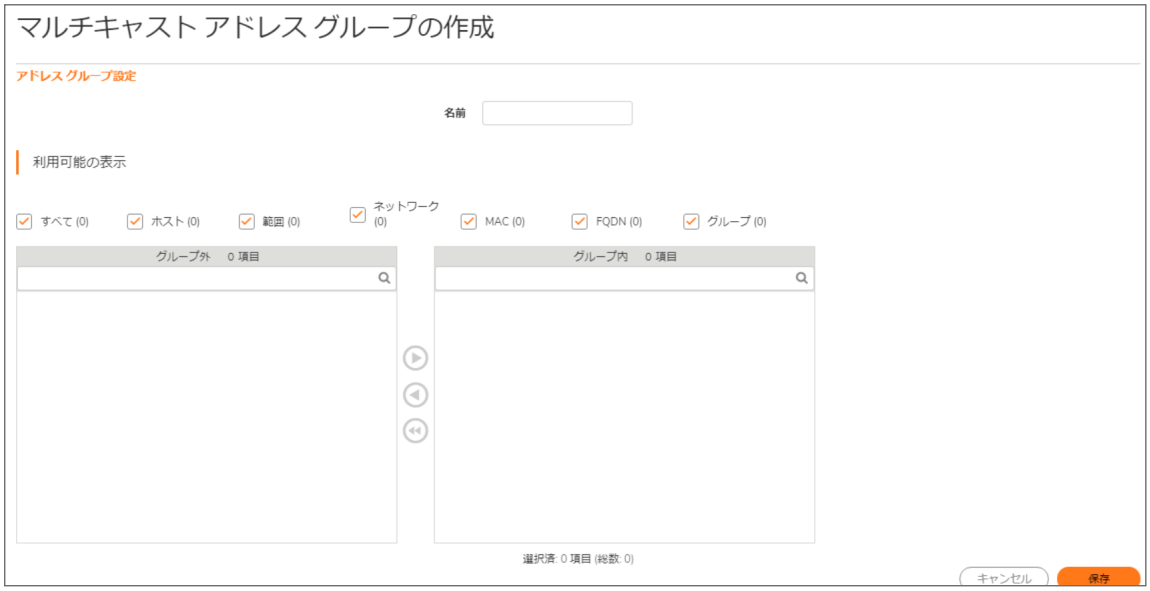
1. 「**以下のマルチキャスト アドレスの受け取りを有効にする**」ドロップダウン メニューで、「**マルチキャスト アドレス オブジェクトの作成**」を選択します。「**マルチキャスト アドレス オブジェクトの作成**」ダイアログが表示されます。

2. 「**名前**」フィールドでアドレス オブジェクトの名前を設定します。
3. 「**ゾーンの割り当て**」ドロップダウン メニューから「**MULTICAST**」を選択します。
4. 「**種別**」ドロップダウン メニューで、「ホスト」、「範囲」、「ネットワーク」、「MAC」、または「FQDN」を選択します。
5. 選択する**種別**に応じて、ダイアログのオプションは変化します。選択した内容によって表示が異なります。

種別	表示されるオプション
ホスト	**IP アドレス** – ホストまたはネットワークの IP アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である 224.0.0.0 ～ 239.255.255.255 の範囲内で指定する必要があります。
ネットワーク	• **ネットワーク** – ホストまたはネットワークの IP アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である 224.0.0.0 ～ 239.255.255.255 の範囲内で指定する必要があります。 • **ネットマスク/接頭辞長** – ネットワークのネットマスクを入力します。
範囲	「**範囲開始**」と「**範囲終了**」に、アドレス範囲の開始アドレスと終了アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である 224.0.0.1 ～ 239.255.255.255 の範囲内で指定する必要があります。
MAC	• **MAC アドレス** – ホストまたはネットワークの MAC アドレスを入力します。 • **マルチホーム ホスト** – MAC アドレスがマルチホーム ホスト用である場合に選択します。このオプションは、既定では選択されています。
FQDN	• **FQDN ホスト名** – ホストの完全修飾ドメイン名を入力します。 • **DNS 登録の TTL の手動設定 … (120~86400 秒)** – DNS 登録の有効期間 (TTL またはホップ制限) を入力する場合に選択します。このオプションは、既定では選択されていません。選択すると、TTL フィールドがアクティブになります。範囲は 120～86400 秒です。

6. 「**保存**」を選択します。

マルチキャスト アドレス グループの作成



- 「**名前**」フィールドにアドレス グループの名前を設定します。
- 「**利用可能の表示**」で、IP をフィルタするオプションとして「すべて」、「ホスト」のみ、「範囲」のみ、「ネットワーク」のみ、「MAC」のみ、「FQDN」のみ、既存の「グループ」、またはこれらの組み合わせを選択します。
- 選択された IP を右側のウィンドウに移動して、選択内容をマルチキャスト アドレス グループに含めます。
- 「**保存**」を選択します。

SNMP 状況

ここでは、IGMP 状態テーブルのフィールドについて説明します。

- 「**マルチキャスト グループ アドレス**」 — インターフェースが属しているマルチキャスト グループ アドレスです。
- 「**インターフェース/VPN トンネル**」 — VPN ポリシーのインターフェース（LANなど）です。
- 「**IGMP バージョン**」 — IGMP バージョン（V2 や V3 など）を示します。
- 「**残り時間**」 — 残り時間の詳細を示します。
- 「**消去**」 — 特定のエントリを消去するためのアイコンが用意されています。
- 「**消去**」および「**すべて消去**」アイコン — 特定の登録を直ちに消去するには、その登録の左側にあるチェックボックスをオンにして、「**消去**」を選択します。すべての登録を直ちに消去するには、「**すべて消去**」ボタンを選択します。

マルチキャストの有効化

このセクションでは、VPN 経由および LAN 専用インターフェースでのマルチキャストの有効化の方法を説明します。

トピック:

- LAN 専用インターフェースでのマルチキャストの有効化
- VPN トンネル経由でアドレス オブジェクトのマルチキャスト サポートを有効にする

LAN 専用インターフェースでのマルチキャストの有効化

ファイアウォールの LAN 専用インターフェースのマルチキャスト サポートを有効化するには、以下の手順を実行します。

1. 「**ネットワーク | システム > マルチキャスト**」ページに移動します。
2. 「**マルチキャスト**」で、「**マルチキャストを有効にする**」を選択します。
3. 「**マルチキャスト ポリシー**」で、「**すべてのマルチキャスト アドレスの受け取りを有効にする**」を選択します。
4. 「**適用**」を選択します。
5. 「**ネットワーク | システム >インターフェース**」ページに移動します。
6. 設定する LAN インターフェースの**編集**アイコンを選択します。「インターフェースの編集」ダイアログが表示されます。
7. 「**詳細**」を選択します。
8. 「**マルチキャスト サポートを有効にする**」を選択します。

9. 「**OK**」を選択します。
10. 「**適用**」を選択します。

VPN トンネル経由でアドレス オブジェクトのマルチキャスト サポートを有効にする

VPN トンネルを使用してオブジェクトのマルチキャスト サポートを有効にするには、以下の手順を実行します。

1. 「**ネットワーク | システム > マルチキャスト**」ページに移動します。
2. 「**マルチキャスト**」で、「**マルチキャストを有効にする**」を選択します。
3. 「**マルチキャスト ポリシー**」で、「**以下のマルチキャスト アドレスの受け取りを有効にする**」ドロップダウン メニューから「**マルチキャスト アドレス オブジェクトの作成**」を選択します。「**マルチキャスト アドレス オブジェクトの作成**」ダイアログが表示されます。

4. 「**名前**」フィールドに、マルチキャスト アドレス オブジェクトの名前を入力します。
5. 「**ゾーンの割り当て**」ドロップダウン メニューから、次のようにしてゾーンを選択します。「DMZ」、「LAN」、「MULTICAST」、「SSLVPN」、「VPN」、「WAN」のいずれかのゾーンを選択します。
6. 「**種別**」ドロップダウン メニューから種別を選択すると、選択内容に応じてその他のオプションが変わります。選択した内容によって表示が異なります。
   - 「**ホスト**」を選択した場合は、「**IP アドレス**」フィールドに IP アドレスを入力します。
   - 「**範囲**」を選択した場合は、「**範囲開始**」フィールドと「**範囲終了**」フィールドに開始アドレスと終了アドレスをそれぞれ入力します。
   - 「**ネットワーク**」を選択した場合は「**ネットマスク**」フィールドにネットワーク IP アドレスを、「**ネットマスク /接頭辞長:**」フィールドにネットマスクまたは接頭辞長を入力します。
   - 「**MAC**」を選択した場合は、「**MAC アドレス**」フィールドに MAC アドレスを入力し、必要に応じて、「マルチホーム ホスト」チェックボックスをオンにします（既定でオンになっています）。
   - 「**FQDN**」を選択した場合は、「**FQDN ホスト名**」フィールドに FQDN ホスト名を入力します。
7. 「**保存**」を選択します。
8. 「**ネットワーク | システム >インターフェース**」ページに移動します。
9. 設定したいグループ VPN ポリシーの**編集**アイコンを選択します。「VPN ポリシー」ダイアログが表示されます。
10. 「**詳細**」を選択します。

11. 「**詳細設定**」セクションで、「**マルチキャスト サポートを有効にする**」を選択します。

12. 「OK」を選択します。

13

ネットワーク監視

トピック:

- ネットワーク監視について
- ネットワーク監視の設定

ネットワーク監視ポリシーについて

ネットワーク パスの性能メトリックは、ネットワーク監視プローブを使用して決定されます。SonicOS は ICMP および TCP プローブ種別をサポートしています。詳細については、「ネットワーク監視ポリシーの設定」を参照してください。

「**ネットワーク | システム > ネットワーク監視**」ページには、アドレス オブジェクト グループ内の各パス（インターフェース）の動的性能データ（待ち時間/ジッタ/パケット損失）とプローブ状況が表とグラフで表示されます。最新 1 分（既定値）、最新 1 日、最新 1 週、または最新 1 月のデータを表示することができます。

#	プローブの番号。「折りたたみ/展開」アイコンは、グラフの表示を切り替えます。
名前	ネットワーク監視ポリシーの名前。
IP バージョン	IPv4 または IPv6
プローブ対象	論理プローブが有効になっている場合、テスト パケットをリモート プローブ対象に送信して、WAN パスの可用性を確認することができます。
ゲートウェイ	トラフィックの送信元となったゲートウェイ。
ローカル IP	選択したアドレス オブジェクト
インターフェース	特定のパス/インターフェースを介して送信されたプローブが、プローブ対象に到達して確認応答が返されるまでの往復の時間（ミリ秒単位）。これは、「ネットワーク監視ポリシー」テーブル内のプローブの登録の下にグラフで表示されます。

プローブ種別	ネットワーク監視の種別 • **Ping** – 明確なルート • **TCP** – 明確なルート ⓘ **補足:** 「TCP – 明確なルート」を「RST 応答を未応答としてカウントする」フィールドとともに選択すると、「ポート」フィールドも使用可能になります。
間隔	SD-WAN 性能プローブの間の時間間隔（秒単位）。
ポート	SD-WAN 性能プローブのポート。指定できる値は、1（最小）～65535（最大）です。ポートは、プローブ種別として「TCP – 明確なルート」を選択した場合にのみ表示されます。プローブ種別が「Ping – 明確なルート」の場合は、ハイフン（–）が表示されます。
応答タイムアウト	応答に対する最大待ち時間。
失敗しきい値	プローブ状況が「休止中」と設定されるまで無応答回数。
成功しきい値	プローブ状況が「稼働中」と設定されるまでの応答回数。
すべて応答が必要	有効または無効
RST 失敗	プローブ種別が「**TCP – 明確なルート**」の場合、RST 応答を失敗としてカウントするかどうか。
状況	監視が稼働中か休止中かを示します。
UUID	UUID/GUID に基づくクライアント識別子
コメント	インターフェース設定時に入力されたコメント。

ネットワーク監視を設定すると、「ネットワーク監視ポリシー」画面で設定したグループが使用するインターフェースごとに既定の行が作成されます。

ネットワーク監視ポリシーの設定

ネットワーク監視ポリシーを追加するには、以下の手順に従います。

1. 「**ネットワーク | システム > ネットワーク監視**」に移動します。
2. 「**+ 追加**」を選択します。「**ネットワーク監視ポリシーを追加する**」ダイアログが表示されます。

3. 「**名前**」フィールドにわかりやすい名前を入力します。
4. 「**プローブ対象**」からアドレス オブジェクトを選択します。
5. 「**プローブ種別**」から、以下を選択します。
   - Ping (ICMP) – **明確なルート**(既定)。ステップ 7 に進みます。
   - TCP – **明確なルート**。「**ポート**」フィールドとその他のオプションが利用可能になります。
6. 明確なルートのポート番号を「**ポート**」フィールドに入力します。
7. 「**ホストのプローブ間隔 … 秒毎**」フィールドにプローブの時間間隔を入力します。最小値は 1 秒、最大値は 3600 秒、既定値は 3 秒です。

   ⓘ | **ヒント:** プローブ間隔は応答タイムアウトより長くなければなりません。
8. 「**応答タイムアウト…秒**」フィールドに、応答の最大遅延を入力します。最小値は 1 秒、最大値は 60 秒、既定値は 1 秒です。

9. 「**次に達したらプローブ状況をダウンさせる...回の失敗した間隔**」フィールドに、性能プローブが「休止中」と設定されるまでの無応答回数の最大数を入力します。最小値は 1、最大値は 100、既定値は 3 です。
10. 「**次に達したらプローブ状況をアップさせる...回の成功した間隔**」フィールドに、性能プローブが「稼働中」と設定されるまでの応答回数の最大数を入力します。最小値は 1、最大値は 100、既定値は 1 です。
11. 「**プローブ種別**」で「**TCP – 明確なルート**」を選択した場合は、「**RST 応答を未応答としてカウントする**」オプションが使用可能になります。RST 応答を欠落間隔としてカウントするオプションを選択してください。このオプションは、既定では選択されていません。
12. 「**すべてのホストが要応答**」オプションを使用して、すべてのホストからの応答の強制を有効または無効にします。
13. (「プローブ種別」が「**TCP –明確なルート**」の場合) RST 応答を未応答としてカウントするかどうか、「**RST 応答を未応答としてカウントする**」を有効または無効にします。
14. 必要に応じて、「**コメント**」フィールドにコメントを入力します。
15. 「**追加**」を選択します。
16. さらにプローブを追加するには、ステップ 3 からステップ 14 を繰り返します。
17. 「**閉じる**」を選択します。

ネットワーク監視ポリシーの削除

ネットワーク監視ポリシーを削除するには、以下の手順に従います。

1. 削除するには:
   ネットワーク監視ポリシーを 1 つ削除する場合は、
   - 「**設定**」列の対応する「**削除**」アイコンを選択します。

     確認メッセージが表示されます。
   - 複数のネットワーク監視ポリシーを削除する場合は、対応するそれぞれの「**選択**」チェックボックスをオンにして「**削除**」を選択します。

     確認メッセージが表示されます。
2. 「**OK**」を選択します。

14

AWS 構成

ファイアウォールとアマゾン ウェブ サービス（AWS）の統合により、AWS CloudWatch ログへのログの送信、EC2 インスタンスへのアドレス オブジェクトとグループの割り当て、仮想プライベート クラウド（VPC）に接続可能な VPN の作成が可能になります。概要と、個々のファイアウォール GUI ページの使用方法を説明するページへのリンクは、『*SonicOS AWS ユーザ ガイド*』を参照してください。

ファイアウォールがアマゾン ウェブ サービス（AWS）のさまざまなアプリケーション プログラミング インターフェース（API）と通信し、それによって AWS との統合を実装できるようにするには、関連する AWS セキュリティ資格情報を使用してファイアウォールを設定する必要があります。必要な情報には、AWS Identity and Access Management（IAM）ユーザのアクセス キー、対応するシークレット アクセス キー、既定の地域が含まれます。既定の地域は、「AWS ログ」ページ、さらに「AWS オブジェクト」ページと「AWS VPN」ページの初期化に使用します（ただし、この 2 つのページでは異なる地域を選択できます）。

AWS セキュリティ資格情報

AWS セキュリティの一般的な機能についてはこの記事では扱いません。AWS のマニュアルはわかりやすく、明瞭で、情報量が豊富です。AWS ユーザは、AWS Identity and Access Management（IAM）の詳細についてよく理解しなければなりません。ここでは、ファイアウォールを SonicOS がサポートする AWS サービスと統合できるようにするために必要な内容についてのみ説明します。

IAM グループとユーザ

AWS マネジメント コンソールの IAM ページで、ユーザおよびグループを含む IAM Identity の作成と管理を行うことができます。

IAM ユーザが存在しない場合、それを作成する必要があります。ファイアウォールは、そのユーザを使用して、自身がサポートするサービスのためにさまざまな AWS の API に接続します（ここでは、AWS アカウントを作成済みであり、ルート アクセス権限または広範な管理者権限を持つ管理者がそのアカウントでログインしていると仮定しています）。

異なるサービスにアクセスするには、特定の権限が必要になります。こうした権限をユーザに直接付与します。または、IAM グループに割り当てたセキュリティ アクセス ポリシーにその権限を適用し、そのグループにユーザを追加します。

使用するセキュリティ ポリシーでは、ユーザが属するグループに適用する、またはユーザに直接適用する場合でも、次の権限を含める必要があります。

AmazonEC2FullAccess	AWS オブジェクトおよび AWS VPN 用
CloudWatchLogsFullAccess	AWS ログ用

グループの作成については、IAM のマニュアルで説明されています。厳密には、グループを作成する必要はありません。権限はユーザに直接割り当てることができますが、一般的には、複数のユーザに使用できるようにグループを定義します。

ユーザを作成する必要があります。ファイアウォールのみで特に使用するためにユーザを作成できますが、同ユーザが AWS マネジメント コンソールにアクセスする場合、関連するチェックボックスをオンにする必要があります。どちらの場合も、ユーザには「プログラム アクセス」が必要です。

「ユーザの追加」ウィザードの 2 番目のステップでは、ユーザをグループに追加する、または権限を直接付与することによってユーザに割り当てる権限を決定します。

作成するユーザの詳細を確認した後、「ユーザの作成」ボタンを押下します。ここで最後に実行する重要な手順があります。

「ユーザの追加」ウィザードを終了せず、次の手順を実行してください。

そのユーザ用に作成された「**シークレット アクセス キー**」を取得する必要があります。**シークレット アクセス キー**は、**アクセス キー**とともに、ファイアウォールの設定に使用します。また、API による AWS へのアクセス時にも常に必要です。シークレット アクセス キーのコピー、またはダウンロードした CSV ファイルを安全な場所に保存してください。

最後に、必要な権限を付与して新規作成したユーザが AWS コンソールの「IAM ユーザ」セクションに表示されます。

シークレット アクセス キーを取得できなかった場合は、IAM コンソールの「ユーザ」セクションから別のアクセス キーを作成できます。これは、アクセス キーをローテーションするのに適した方法と考えられています。

ファイアウォール設 定

ファイアウォールが AWS API にアクセスできるようにするためのユーザ アカウント用のアクセス キーとシークレット アクセス キーを取得していれば、ファイアウォールの基本設定自体は簡単です。

1. 「**ネットワーク | システム > AWS 構成**」に移動します。

2. アクセス キー ID とシークレット アクセス キーを入力し、確認して、既定の地域を選択します。
   既定の地域は「AWS オブジェクト」ページと「AWS VPN」ページの初期化にのみ使用します。ただし、この地域はファイアウォール イベント ログを AWS CloudWatch ログに送信する際に使用されるので、「AWS ログ」ページの変更に影響を受けます。

すべての設定を入力した後、「**適用**」を選択して構成を保存します。

接 続のテスト

送信される資格情報が受け入れ可能か、またファイアウォールが AWS と正常に通信できるかをテストするには、「**接続のテスト**」を選択します。すると、ファイアウォールから実行中のテストの数とフィードバックが表示されます。

例えば、無効なアクセス キーが入力されていたとすると、結果としてポップアップ ダイアログに次のように表示されます。

「**接続のテスト**」を選択すると、実施したテストに関する詳細情報が表示され、失敗したタスクが強調表示されます。

一連のポップアップ ダイアログを閉じ、無効なアクセス キーを修正し、新しい設定を保存した後で、「接続のテスト」を再度実行することができます。成功した場合、ポップアップ ダイアログにはその旨が表示されます。

AWS 資格情報の設定が完了しました。ファイアウォールの設定に進み、「AWS ログ」ページでログ イベントを AWS CloudWatch ログに送信したり、「AWS オブジェクト」ページで EC2 インスタンスをアドレス オブジェクトやアドレス グループにマッピングしたり、「AWS VPN」ページでファイアウォールを仮想プライベート クラウドに接続することができます。

15

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。
- にアクセスする https://mysonicwall.com。
- 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 システム 管理ガイド
更新日 – 2021 年 1 月
ソフトウェア バージョン – 7
232-005452-10 Rev A

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