SonicOS 7

スイッチ ネットワーク

管理者ガイド

SONICWALL®

目次

1

概要

トピック:

- 事前計画: スイッチ追加前
- 物理表示: スイッチの有効化
- 一覧表示: ポートの設定
- 概要: スイッチ詳細の確認

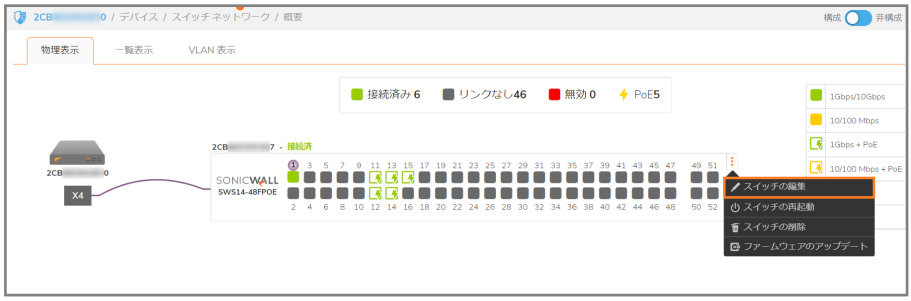
スイッチ追加前

- 最初に MySonicWall でスイッチを必ず登録してください。
- 実装するファイアウォール/スイッチのトポロジを検討してください。『*スイッチ入門ガイド*』を参照してください。ダウンロード場所: https://www.sonicwall.com/ja-jp/support/technical-documentation
- スイッチを手動で追加する場合は、最初に工場出荷時の構成になっているか確認してください。確認するには、リセット スイッチを 10 秒間押し下げるか、スイッチのローカル UI、またはコマンド ライン インターフェースを使用します。
- 管理リンクをスイッチに手動で追加する場合、DHCP リース レンジが既定の管理 IP アドレスをサポートしていることを確認してください。詳細については、「スイッチ管理ポートをファイアウォールに接続する」を参照してください。
- スイッチ インターフェースにリンクしているファイアウォール インターフェースでは、「**SonicWall スイッチの自動検出を有効化**」オプションが有効になっている必要があります。ファイアウォール インターフェースを編集し、「**インターフェースの編集**」ダイアログの「**詳細**」画面でこのオプションを有効にしてください。
- スイッチ インターフェースにリンクしているファイアウォール インターフェースは、PortShield ホストにはできません。また、他のファイアウォール インターフェースをそれに対してポストシールドすることもできません。スイッチ インターフェースにリンクしているファイアウォール インターフェースは、PortShield グループ メンバーにはできません。つまり、別のファイアウォール インターフェースに対してポストシールドすることはできません。
- スイッチは、手動またはゼロタッチでデイジーチェーン構成に追加できます。
- スイッチをデイジーチェーン接続する場合、十分な容量を持った共通リンク（管理およびデータ）をセットアップすることを検討してください。ファイアウォールから親スイッチへの接続を構成することなく、追加で接続を確率しないでください。スイッチを追加するときは、ファイアウォールからスイッチへの他の接続を確立してください。
- スイッチとファイアウォールを結ぶ管理リンクがデータ トラフィックから孤立する場合、スイッチは静的 IP アドレスで構成する必要があります。

- SonicWall スイッチを追加する前に、ファイアウォール インターフェースに予約済みの VLAN レンジ内で変更を加えてください。スイッチの接続後に予約済みの VLAN レンジを変更する場合、スイッチの接続を解除してから再追加する必要があります。
- スイッチを高可用性 (HA) ペアに追加する場合:
    - ゼロタッチでスイッチを HA ペアに追加することはできません。
    - HA でスイッチを使用するには、最初に HA ペアを作成し、その次にスイッチを手動で追加する必要があります。

スイッチの有効化

スイッチがオフラインの場合、「**デバイス > スイッチ ネットワーク > 概要**」に移動し、オフラインのスイッチの 3 ドット メニューをクリックして、「スイッチの編集」をクリックすると、「スイッチ設定」ダイアログ ボックスが開きます。スイッチの設定の詳細 (IP アドレス、シリアル番号、スイッチ管理インターフェース) が正しいか確認してください。

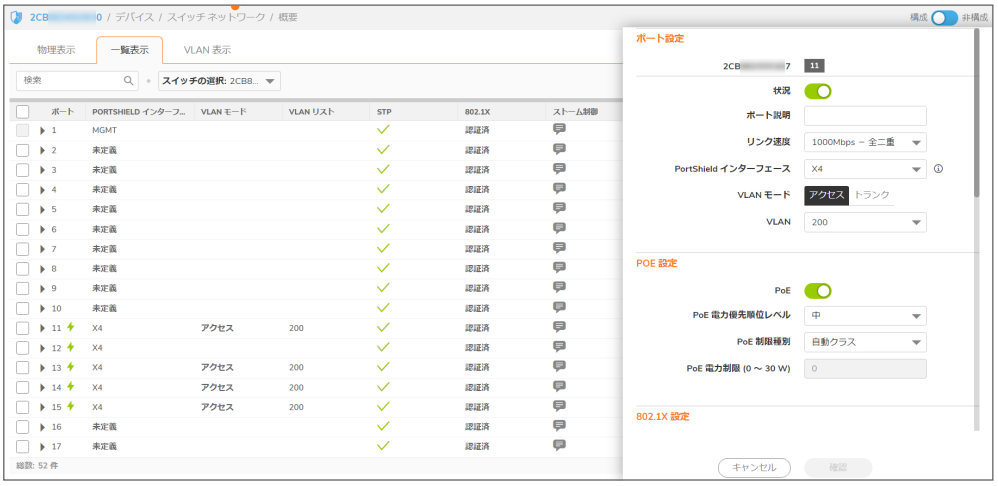


ポートの設定

特定のポートを構成するには、以下の手順に従います

1. 「**デバイス > スイッチ ネットワーク > 概要**」に移動します。
2. 以下のいずれかを実行します。
   - 「**物理表示**」にある目的のポートをクリックします。

   - 「**リスト表示**」をクリックし、目的のポートを選択して「**編集ポート**」鉛筆アイコンをクリックします。



特定のポートに関するポート設定ダイアログは、画面右側に表示されます。

3. ポートの次のオプションを構成します。

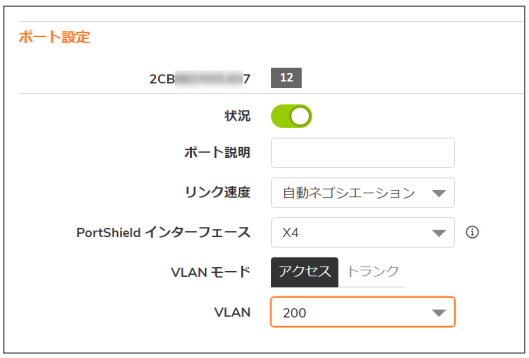
ポート設定:

- **状況** – スライダーをクリックして有効/無効にします。
- **ポート説明** – このポートの説明を入力します。
- **リンク速度** – 既定では「**自動ネゴシエーション**」です。「**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**」も選択できます。
- **Portshield インターフェース** – ファイアウォール インターフェースに対してスイッチ ポートをポートシールドするには、このオプションを設定します。既定では「**未定義**」です。「**すべて**」および「**X0–Xn**」を選択できます。
- **専用 PortShield アップリンク** – 「**PortShield インターフェース**」が任意のゾーン内のファイアウォール インターフェースに対して設定されている場合、このオプションが表示されます。スライダーをクリックして有効/無効にします。

- **VLAN モード** – VLAN 副インターフェースを使用して構成されるインターフェースに対して「**PortShield インターフェース**」が設定されている場合、このオプションが表示されます。既定では「**アクセス**」です。

  ポートが特定の VLAN 上でデータを転送する場合は、「**アクセス**」を選択します。

  複数の VLAN に対してトラフィックを伝送できるポートには、「**トランク**」を選択します。ポート トランキングを利用すると、複数の物理リンクを 1 つの論理リンクに割り当て、1 つの高速リンクとして機能するようにすることで、帯域幅を劇的に増大させることができます。「ポート トランキング」を利用して複数の接続をとりまとめ、1 本の太めの “パイプ” のように帯域幅を組み合わせます。



- **ネイティブ VLAN** – 「**VLAN モード**」に「**トランク**」が選択されている場合、「**ネイティブ VLAN**」フィールドが表示されます。「**ネイティブ VLAN**」フィールドに 1 ～ 4094 の数字を入力し、ポートのネイティブ VLAN (Port VLAN ID) を割り当てます。

  「ネイティブ VLAN」オプションを選択すると、VLAN タグを伝送しないトラフィックにスイッチ ポート VLAN ID を指定できます。これは、SonicWave のプロビジョニングに役立ちます。所定のスイッチ

ポートで受信したパケットには、そのポートのネイティブ VLAN ID が割り当てられ、パケットの送信先アドレスに対応するポートに転送されます。パケットを受信したポートのネイティブ VLAN が、パケット転送用ポートのネイティブ VLAN とは異なる場合、スイッチはパケットを破棄します。

- **VLAN** – 「**VLAN モード**」に連動して「**VLAN**」フィールドが表示されます。「**未定義**」か、「**PortShield インターフェース**」で選択したファイアウォール インターフェースに関連付けられた VLAN 副インターフェースの数を選択します。

PoE 設定: PoE 対応スイッチ上のポートは、Power over Ethernet により接続デバイスへ給電できます。

- **PoE** – スライダーをクリックしてこのポートで Power over Ethernet を有効/無効にします。
- **PoE 給電優先順位レベル** – 既定では「**中**」です。「**重大**」、「**高**」、「**低**」を選択できます。複数のデバイスが接続され、スイッチの PoE 容量を超える場合、優先順位レベルが給電先のポートを決定します。
- **PoE 制限種別** – 既定では「**自動クラス**」で、デバイス ディスカバリ プロトコルを使用し、接続デバイスを検出してその種別を学習します。「**ユーザ定義**」を選択することもできます。
- **PoE 給電制限 (0–30 W)** – 上で「**自動クラス**」を選択した場合、このフィールドは無効です。「**ユーザ定義**」を選択した場合は、ポート給電制限ワット数を 0 から 30 の値で入力してください。

  SonicWall スイッチ モデルごとに合計電力予算は異なります。

  - SWS12-8POE – 55 ワット (IEEE802.3 af のみをサポート)
  - SWS12-10FPOE – 130 ワット (IEEE802.3 af および at)
  - SWS14-24FPOE – 410 ワット (IEEE802.3 af および at)
  - SWS14-48FPOE – 730 ワット (IEEE802.3 af および at)

802.1X 設定: IEEE 802.1X は、LAN または WLAN にアクセスするポートに接続しようと試みるユーザまたはデバイスの認証制御を定義します。

- **モード** – 既定では「**承認済みを強制**」です。「**自動**」および「**未承認を強制**」を選択できます。
- **ゲスト VLAN** – スライダーをクリックして有効/無効にします。既定は「無効」です。
- **RADIUS VLAN 割り当て** – スライダーをクリックして有効/無効にします。ユーザの資格情報または証明書に基づいてユーザの ID を RADIUS サーバによって確認できます。RADIUS サーバは、スイッチ ポートの VLAN 割り当てを担当します。

詳細設定:

- **STP** – スライダーをクリックして有効/無効にします。ポートの STP 設定を構成する前に、スイッチで Spanning Tree Protocol (STP) を有効にする必要があります。ネットワーク内に冗長パスがあるとき、STP はループを防止します。
- **ポート隔離** – スライダーをクリックして有効/無効にします。有効にするとポートは隔離されます。

- **ポート セキュリティ最大カウント** – 既定では「**0**」で、ポート セキュリティは無効です。範囲は 0 ～ 256 です。これは、ポートで学習可能な MAC アドレスの最大数です。特定ポートでのアクセスを特定の MAC アドレスを持つユーザに制限することで、ネットワーク セキュリティを向上させることができます。
- **B/W 受信速度 (Kbps)** – 既定では「**0**」で、受信帯域幅制御は無効です。許容値は、0 ～ 1,000,000 の 16 の倍数です。
- **B/W 送信速度 (Kbps)** – 既定では「**0**」で、送信帯域幅制御は無効です。許容値は、0 ～ 1,000,000 の 16 の倍数です。

音声 VLAN 設定:

- **音声 VLAN 状態** – スライダーをクリックして有効/無効にします。
- **音声 VLAN CoS モード** – 既定では「**送信元**」です。サービス クラス モードには、「**送信元**」または「**すべて**」を選択できます。

QoS 設定: サービス品質 (QoS) により、音声/ビデオ ストリーミングなどの特定の種別のトラフィックに優先順位を付けることができます。

- **信頼** – スライダーをクリックして、受信パケットの信頼モードを有効/無効にします。これを有効にすると、IEEE 802.1p 標準に基づいて (8 つの CoS 優先順位タグを使用して) トラフィックを分類できます。
- **CoS** – CoS 優先順位を選択し、このポートに入ってくるパケットの優先順位を設定します。既定は「**0**」です。サービス クラス タグの範囲は 0 ～ 7 です。0 (バックグラウンド)、1 (ベスト エフォート) はトラフィック転送キュー内の優先順位が最低で、7 は優先順位が最高です。

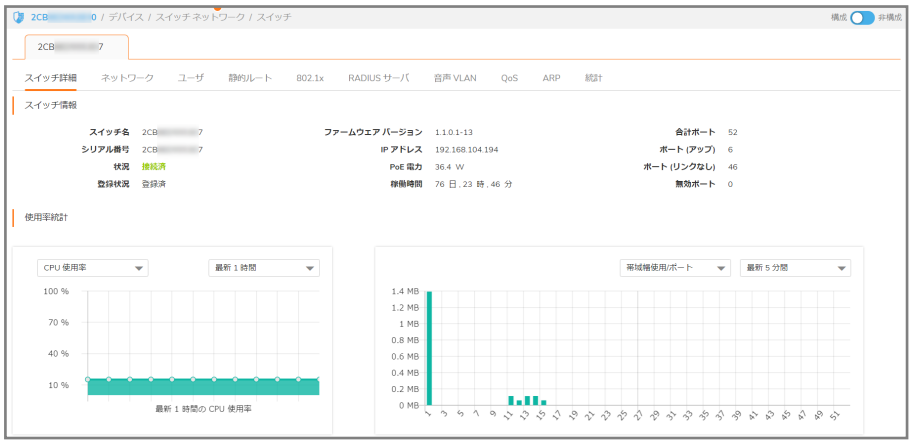
ストーム制御設定: ストーム制御は、スイッチによって受け入れられ転送されるブロードキャスト フレーム、未定義のマルチキャスト フレーム、未定義のユニキャスト フレームの量を制限します。ストーム制御をポートごとに有効にするには、パケット タイプおよびパケット転送速度を定義します。速度が定義された速度を超えると、スイッチはフレームを破棄します。

- **ブロードキャスト速度 (Kbps)** – 既定では「**0**」で、ポート ブロードキャストは無効です。許容値は、0 ～ 1,000,000 の 16 の倍数です。
- **未定義のマルチキャスト速度 (Kbps)** – 既定では「**0**」で、ポートの未定義のマルチキャストは無効です。許容値は、0 ～ 1,000,000 の 16 の倍数です。
- **未定義のユニキャスト速度 (Kbps)** – 既定では「**0**」で、ポートの未定義のユニキャストは無効です。許容値は、0 ～ 1,000,000 の 16 の倍数です。

4. 「**確認**」をクリックして変更を保存して適用するか、「**キャンセル**」をクリックして保存せずに編集ダイアログを閉じます。

スイッチ詳細の確認

「**デバイス > スイッチ ネットワーク > スイッチ > スイッチ詳細**」へと移動し、ファイアウォールに接続されたスイッチに関するサマリを取得します。



2

ファイアウォールから管 理

トピック:

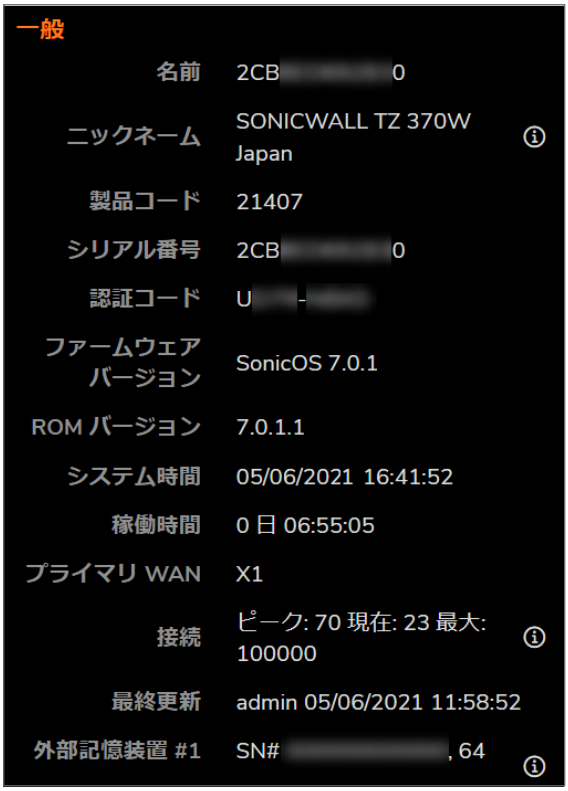
ゼロタッチによるファイアウォールへのスイッチ追加

ⓘ **重要:** 重要: スイッチをファイアウォールに追加する前に、スイッチの登録を行ってください。

ⓘ **補足:** ファイアウォールがスイッチの存在を検知するためには、ファイアウォールがゼロタッチでスイッチを追加するようにセットアップする必要があります。

ファイアウォールを準備するには、以下の手順に従います

1. 「**ホーム > ダッシュボード > システム > デバイス**」に移動し、ファイアウォールの**ファームウェア バージョン**が最新レベルであるか確認してください。

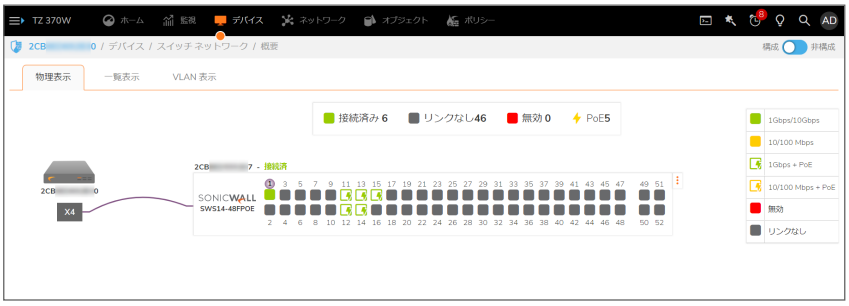


2. スイッチに接続するファイアウォール上のインターフェースを選択します。「**ネットワーク > システム > インターフェース > インターフェース設定**」に移動し、インターフェースを選択して鉛筆アイコンをクリックします。
3. 「**編集インターフェース**」ダイアログ ボックスで、「**詳細**」タブを選択し、「**SonicWall スイッチの自動検出を有効にする**」オプションを有効にして「**OK**」をクリックします。
4. スイッチを選択したファイアウォール インターフェースに接続します。

5. 「**ネットワーク > システム > DHCP サーバ**」に移動し、選択したインターフェースに接続されるスイッチに対してリース スコープが正しいことを確認します。

6. 「**デバイス > スイッチ ネットワーク > 概要**」に移動します。「**許可**」ボタンをクリックしてスイッチをファイアウォールに追加します。

7. ネットワークトポロジがディスプレイの「**概要 > 物理表示**」に表示されます。



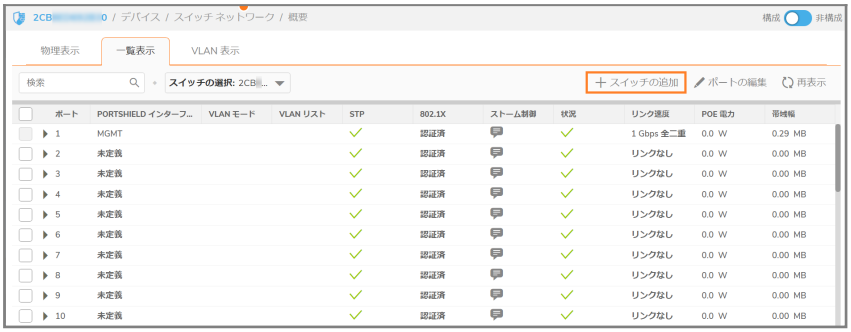
手動によるファイアウォールへのスイッチ追加

1. SonicWall スイッチのポートを、ファイアウォールの利用可能なポートに接続します。RJ45 ポートに接続する場合は CAT5e または CAT6 ケーブル（つまり、RJ45–RJ45）を使用し、対応 SFP インターフェースに接続する場合は光ファイバー ケーブルを使用します。

ⓘ **補足:** スイッチを手動で追加する場合は、最初に工場出荷時の構成になっているか確認してください。確認するには、リセット スイッチ ボタンを 10 秒以上押し下げてください。スイッチが工場出荷時の設定になっているか確認するには、スイッチのローカル UI、またはコンソール ポートからアクセス可能なコマンド ライン インターフェースを使用することもできます。

ⓘ **補足:** ファイアウォールで予約済みの VLAN レンジを変更するには、SonicWall スイッチを追加する前に行ってください。スイッチの接続後に予約済みの VLAN レンジを変更する場合、スイッチの接続を解除してから再追加する必要があります。

2. SonicOS 管理インターフェースにログインし、「**デバイス > スイッチ ネットワーク > 概要 > リスト表示**」に移動します。下に示すように「**スイッチの追加**」をクリックします。



「**スイッチの追加** 」ダイアログが表示されます。

3. 「**スイッチの追加**」ダイアログ ボックスで、以下のフィールドを設定します。

- **スイッチ モデル** – ドロップダウン リストから SWS モデルを選択します。
- **シリアル番号:** – スイッチ底面のラベルに記載されているシリアル番号を入力します。
- **スイッチ名** – スイッチのわかりやすい名前を入力します。
- **コメント** – コメントを入力します。コメントはスイッチを追加するときに必要です。
- **IP アドレス** – スイッチの IP アドレスを入力します。既定では 192.168.168.169 です。

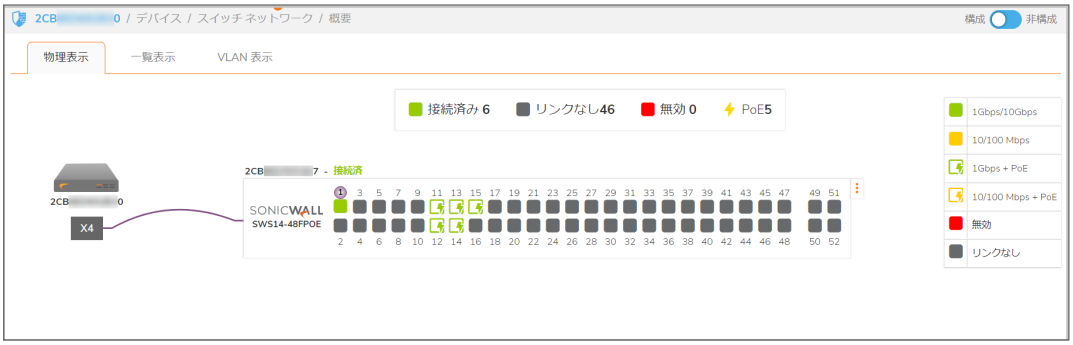
- **ユーザ名** – 既定では *admin* です。
- **パスワード** – 既定では *password* です。
- **スイッチ モード** –単体のスイッチの場合は「**スタンドアロン**」を選択し、同じポートに接続されている複数のスイッチのいずれかの場合は「**デイジーチェーン**」を選択します。
- **スイッチ管理** – スイッチの管理用ファイアウォールに接続されているスイッチ ポートの数を選択します。
- **ファイアウォール アップリンク**: スイッチに接続されているファイアウォール上のインターフェースを選択します。
- **スイッチ アップリンク**: ファイアウォールに接続されているスイッチ ポートの数を選択します。

  ⓘ **補足:** 「ファイアウォール アップリンク」インターフェースと「スイッチ アップリンク」ポートは物理的に相互接続されます。「基本トポロジの設定」セクションの「**アップリンク インターフェースの概要**」を参照してください。

「**詳細設定**」で、スパニング ツリーとジャンボ フレームのサイズ設定を構成します。

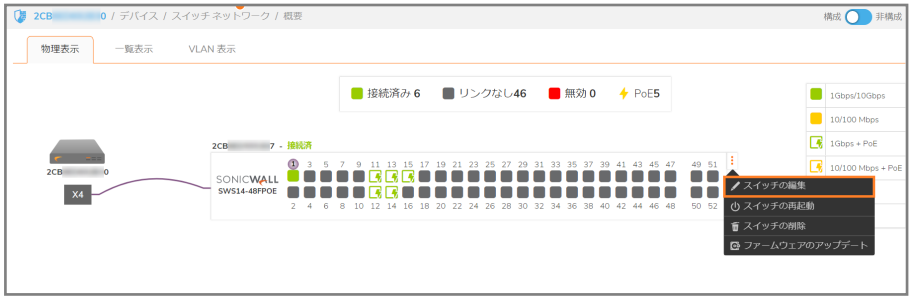
- **STP** – スライダーをクリックして Spanning Tree Protocol を有効/無効にします。
- **STP モード** – 「**高速**」または「**複数**」を選択します。既定では「**複数**」です。
- **ジャンボ フレーム サイズ** – 1522 ～ 10240 の値を入力します。既定では 1522 です。既定値は最大標準送信単位サイズ (バイト) です。この値より大きいフレーム サイズはジャンボとなります。

4. 「**適用**」を選択します。
5. 「**概要 > 物理表示**」にアクセスすると、新しいスイッチが、スイッチとファイアウォールをリンクしているポートと共にグラフィックで表示されます。



スイッチ設定の変更

スイッチ構成を編集するには、3 点ドット メニューをクリックして「**スイッチの編集**」を選択します。



「スイッチの編集」ダイアログ ボックスが表示されます。

ファームウェアのアップグレード

ファームウェアをアップグレードするには、「**概要 > 物理表示**」へ移動し、スイッチ グラフィックの右側にある 3 点ドット アイコンをクリックします。

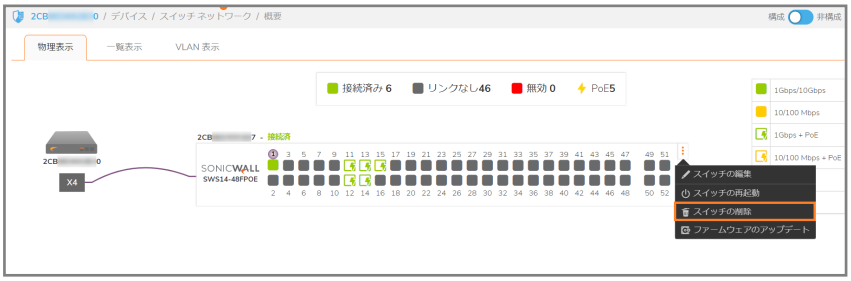
更新アイコンをクリックすると、新しい更新プログラムが利用可能であるかどうかが表示されます。

新しいファームウェアが利用可能であるかどうかを確認してください。利用可能である場合、選択して「アップグレード」をクリックします。

スイッチのシャットダウン

ファイアウォールからスイッチを削除するには、以下の手順に従います

1. 「**デバイス > スイッチ ネットワーク > 概要**」に移動します。
2. 「**スイッチの削除**」をクリックします。



スイッチの再起動

スイッチを再起動するには、以下の手順に従います

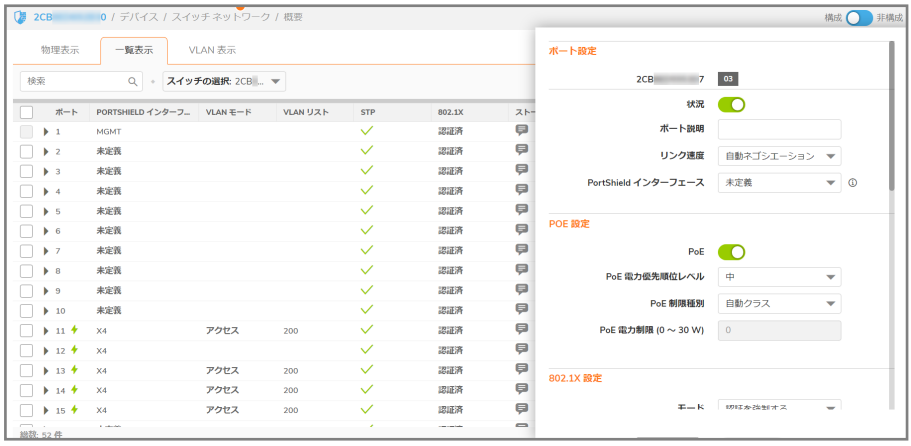
1. 前面パネルの埋込スイッチを 1 秒間押します。

または

1. 「**概要**」ページのスイッチ画像の 3 点メニューをクリックし、「**スイッチの再起動**」をクリックします。

PoE のセットアップ

ポートごとに PoE 制限をセットアップするには、「**デバイス > スイッチ ネットワーク > 概要**」に移動し、「**リスト表示**」をクリックします。PoE をセットアップするポートの編集ボタンをクリックします。PoE 設定が表示されるまで、ポート設定パネルを下へスクロールします。



PoE+ スイッチは、IEEE 802.3af および 802.3at の定義に従って Power over Ethernet (PoE) をサポートします。SWS12-8 PoE 対応スイッチは、-af 標準をサポートし、ポートごとの最大電力は 15.4 ワットです。SWS12-10 および SWS14 シリーズ PoE 対応スイッチがサポートする電力は、ポートごとに 30 ワットです。

スイッチは、標準的な PSE (給電側デバイス) ピン配列に従います。つまり、ピン 1、2、3 および 6 を介して給電されます。

- PoE 管理状況:
- 有効 – デバイス ディスカバリ プロトコルを有効にし、PoE モジュールを使用してデバイスに給電します。デバイス ディスカバリ プロトコルにより、デバイスはデバイス インターフェースに接続された受電デバイスを検出し、その分類を学習します。
- 無効 – デバイス ディスカバリ プロトコルを無効にし、PoE モジュールを使用してデバイスに給電することを停止します。
- PoE 優先順位

給電が弱い場合は、ポート優先順位を選択します。このフィールドの既定は「中」です。例えば、使用率 99% で電源が稼働中で、ポート 1 の優先順位が「高」、ポート 6 の優先順位が「低」の場合、ポート 1 の受電が優先されますが、ポート 6 の受電は拒否される可能性があります。このフィールドに設定できる値は以下のとおりです。4.

- 低 – PoE 優先順位レベルを「低」に設定します。
- 中 – PoE 優先順位レベルを「中」に設定します。
- 高 – PoE 優先順位レベルを「高」に設定します。
- 重大 – PoE 優先順位レベルを「重大」に設定します。
- PoE 電力制限種別
- 自動クラス – ポートごとに 15.4 または 30 W
- ユーザ定義 – ポートからの最大給電量を設定します。

ⓘ | **補足:** ユーザ電力制限は、「自動クラス」値が「ユーザ定義」に設定されている場合にのみ実装できます。

VLAN の追加

仮想 LAN (VLAN) は、トラフィックの管理、セキュリティ、運用を向上させるために、レイヤ 2 スイッチ上で論理イーサネット セグメントを形成するポートの集まりです。VLAN は、物理的レイアウトではなく、論理スキームに従って構成されるネットワークトポロジです。VLAN を使用すると、物理的な場所ではなく、論理機能によってユーザをグループ化できます。すべてのポートは相互に頻繁な通信を行い、ネットワーク内の場所に関係なく、同一の VLAN に割り当てられます。VLAN を利用して、ネットワークを論理的に個別のブロードキャストドメインに分割し、関連機能を持つポートを、同一スイッチ上で個別の論理 LAN セグメントにグループ化できます。これにより、ブロードキャスト パケットを VLAN 内のポート間のみに転送することが可能になるため、ブロードキャスト パケットが 1 つのスイッチ上の全ポートに送信されることはありません。VLAN は、ブロードキャストをより小さく管理しやすい論理ブロードキャストドメインに制限することで、ネットワーク パフォーマンスも増大させます。トラフィックを特定のブロードキャストドメインに制限することで、VLAN はセキュリティを向上させます。

ネットワーク内の各 VLAN には VLAN ID が割り当てられ、VLAN で転送されるパケットのレイヤ 2 ヘッダーの IEEE 802.1Q タグに表示されます。IEEE802.1Q 仕様は、VLAN メンバーシップ情報をイーサネット フレームにタグ付けるための基準方式を確立するものです。IEEE802.1Q の機能を実行するための鍵は、そのタグ内に格納されています。802.1Q 対応スイッチ ポートは、タグ付き/タグなしのフレームを転送するように構成できます。VLAN 情報を格納しているタグ フィールドは、イーサネット フレームに挿入できます。802.1Q VLAN 構成を使用する場合、ポートを VLAN グループの一部になるように構成してください。ポートが VLAN グループのタグ付きデータを受信すると、そのデータはポートが VLAN グループのメンバーにならない限り破棄されます。

ⓘ **重要:** ファイアウォールで予約済みの VLAN レンジに変更を加えるには、SonicWall スイッチを追加する前に行ってください。スイッチの接続後に予約済みの VLAN レンジを変更する場合、スイッチの接続を解除してから再追加する必要があります。

VLAN インターフェースの追加

VLAN を追加するには、ファイアウォールへのアップリンクの下に仮想インターフェースを追加します。

1. 「**デバイス > スイッチ ネットワーク > スイッチ > ネットワーク**」に移動します。
2. 「**ネットワークの追加**」をクリックします。

3. **VLAN ID、アドレス、サブネット マスク**を定義し、アドレス割り当て方式（「**静的**」または「**DHCP**」）を選択します。
4. 「**OK**」を選択します。

音声 VLAN の設定

ⓘ **補足:** 音声 VLAN は、「**デバイス > スイッチ ネットワーク > スイッチ > 音声 VLAN**」表示で、ポートごとに有効/無効にできます。

1. 音声 VLAN を構成するには、「**デバイス > スイッチ ネットワーク > スイッチ**」に移動し、「**音声 VLAN**」をクリックします。

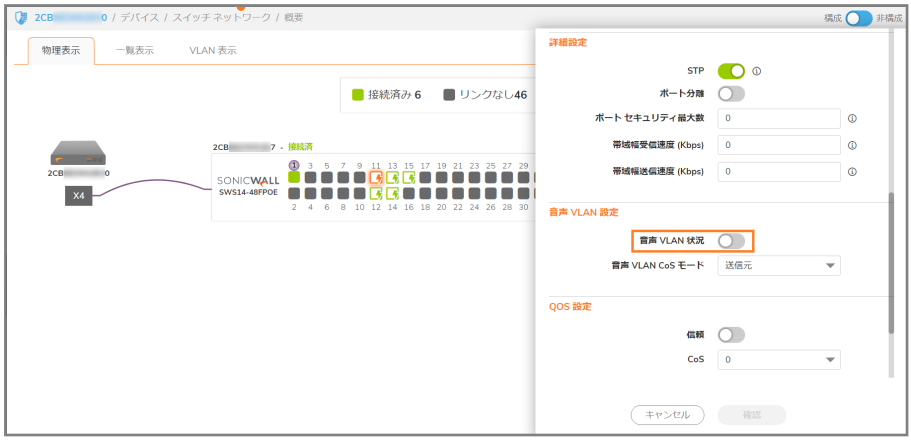
2. 状態を「無効」から「自動」へ移行して音声 VLAN をセットアップし、他のパラメータを設定してから、ディスプレイの下部に表示される「適用」をクリックします。
    - **音声 VLAN ID** – LAN を識別します。
    - **音声優先順位タグ** – 実行中の音声ストリーム間の優先順位を決定します。
    - **DSCP (Differentiated Services Code Point)** – QoS を定義します。

「音声 VLAN 設定」を使用して、音声トラフィック管理を有効にし、「サービス クラス（CoS）」キューをすべてのポートに対して定義するか、送信元の音声トラフィックのみに対して定義するかを決定します。CoS 定義に関する詳細は、QoS のセットアップ.を参照してください。

ⓘ **補足:** スイッチは、各設定による定義に従って、受信音声 VLAN トラフィック タグを認識し、音声優先順位と DSCP を設定します。

物理表示で音声 VLAN を有効/無効にするには、以下の手順に従います

「**デバイス > スイッチ ネットワーク > 概要**」に移動し、ポートをクリックします。サイドバンド ディスプレイが表示され、下に示すように音声 VLAN 状態までスクロールします。



静的ルートの追加

静的ルートをスイッチに追加するには、以下の手順に従います

1. 「**デバイス > スイッチ ネットワーク > スイッチ**」へ移動し、「**静的ルート**」を選択して、「**静的ルートの追加**をクリックします。

2. ダイアログ ボックスを記入します。
   - **送信先 IP** アドレス（最終オクテットを ‘0’ にする: x.x.x.0）。
   - 送信先の**サブネット** マスク。
   - **ゲートウェイ**: スイッチから送信先までの IP アドレス ゲートウェイ。
3. 「**OK**」を選択します。

DNS の編集

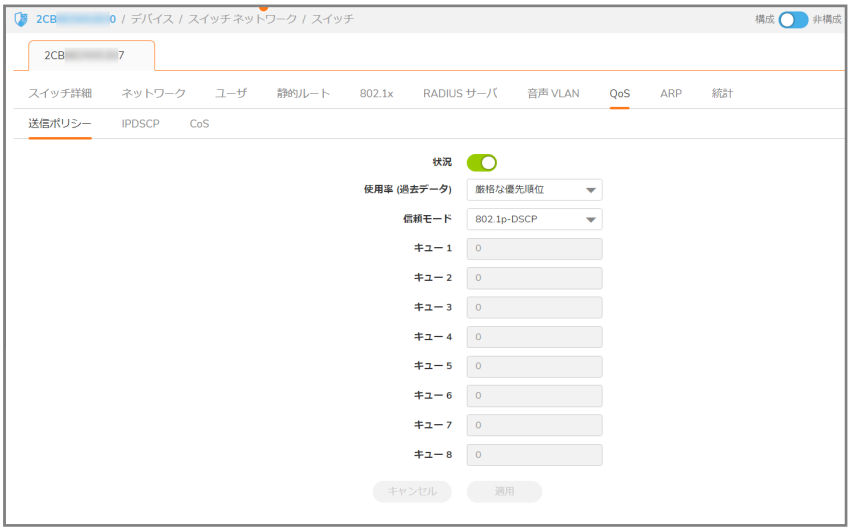
DNS アドレスを設定するには、「**デバイス > スイッチ ネットワーク > スイッチ**」にアクセスして「**ネットワーク**」を選択し、「**DNS**」をクリックします。

QoS のセットアップ

サービス品質（QoS）は、ネットワーク内で優先順位キューを実装する機能を提供します。QoS により、過剰なブロードキャストやマルチキャストを最小限に抑えながら、トラフィックに優先順位を付けることができます。遅延を最小限に抑える必要がある音声やビデオ ストリーミングなどのトラフィックは、高い優先順位のキューに割り当て、その他のトラフィックはより優先順位の低いキューに割り当てると、動作が妨げられることがなくなります。

スイッチに QoS をセットアップするには、以下の手順に従います

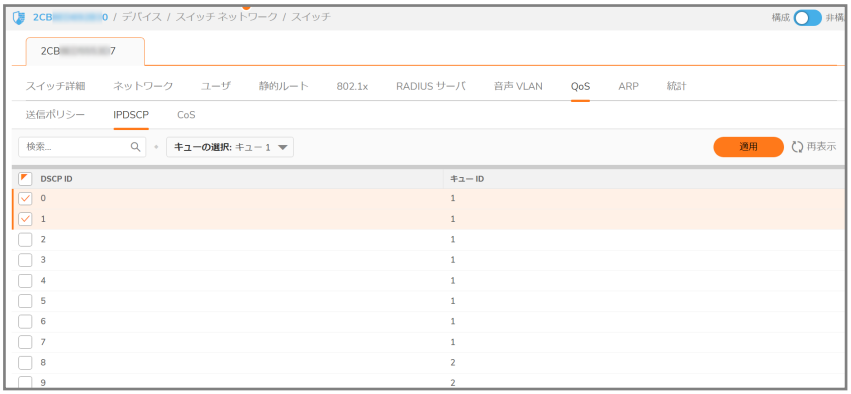
1. 「**デバイス > スイッチ ネットワーク > スイッチ**」に移動し、「**QoS**」をクリックします。



2. 送信ポリシーを設定します。

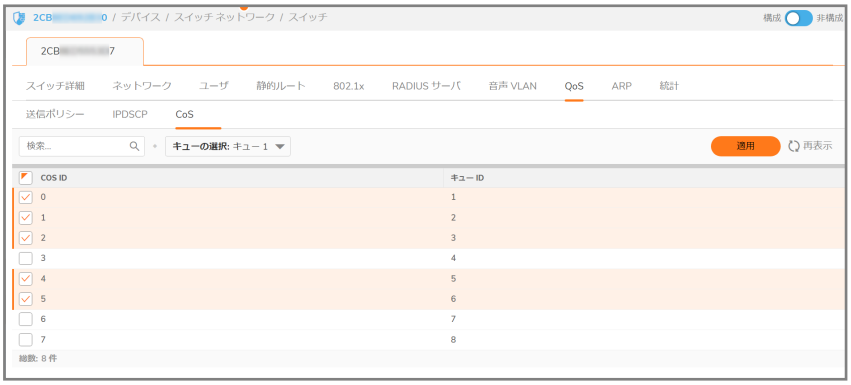
   最初の画面に表示される送信ポリシーは、パケットおよびトラフィックの分類に対するすべてのアプローチに適用されます。前の UI 画面で、状況スライダーを使用して QoS の有効（右側）または無効（左側）を指定できます。スケジュール方法は、キュー番号に基づく厳格な優先順位または重み付きラウンド ロビン（WRR）として設定できます。パケットの分類は、802.1p または DSCP（Differentiated Sevices Code Point）として、あるいは両方として設定できます。

3. 「**IPDSCP**」画面を選択し、DSCP コードを特定のキューに設定します。



4. サービスのクラスを設定するには、「**CoS**」をクリックします。

   CoS（サービスのクラス）画面では、CoS 優先順位タグの値（0 が最低、7 が最高）は、8 個のトラフィック優先順位キュー（最低 1 ～ 最高 8）に関連付けられます。



ユーザのセットアップ

アクセス レベル（管理者とユーザ）が異なるユーザを定義するには、「**デバイス > スイッチ ネットワーク > スイッチ**」へ移動して「**ユーザ**」をクリックします。

「ユーザ レベル権限」を持つユーザは、非設定モードに限定されます。

802.1X 認証のセットアップ

IEEE-802.1X 認証は、RADIUS サーバによるネットワーク アクセス制御のセキュリティ基準を提供し、認証が完了するまでネットワーク ポートの接続を解除した状態を保ちます。802.1X 認証では、サプリカントがユーザ名、パスワード、デジタル証明書などの資格情報を認証システムに提供すると、認証システムは確認のために資格情報を認証サーバに転送します。資格情報が有効であると認証サーバが判定すると、サプリカント（クライアント デバイス）はネットワークの保護された領域に配置されたリソースにアクセスすることを許可されます。スイッチは 802.1X を使用して、ポート アクセス制御の有効化/無効化、ゲスト VLAN の有効化/無効化、EAPOL（Extensible Authentication Protocol over LANs）フレーム転送の有効化/無効化を実行します。

802.1 認証を有効にするには、以下の手順に従います

1. 「**デバイス > スイッチ ネットワーク > スイッチ**」へ移動し、「**802.1 x**」をクリックします。
2. 状況スライダーを右へセットすると、認証が有効になります。その他の設定は以下のとおりです。
    - ゲスト VLAN – スイッチでゲスト VLAN の有効/無効を切り換えます。既定は「無効」です。
    - ゲスト VLAN ID – 現在定義されている VLAN のリストからゲスト VLAN を選択します。

RADIUS サーバを有効にするには、以下の手順に従います

1. 「**デバイス > スイッチ ネットワーク > スイッチ**」で、「**RADIUS サーバ**」をクリックします。「**RADIUS サーバ**」画面で、「**+ 追加**」をクリックします。
2. RADIUS サーバを有効にするには、「**認証済みポート**」を「1812」に設定します。

スイッチのデイジーチェーン

スイッチには、スタンドアロン構成またはデイジーチェーン構成でファイアウォールをセットアップできます。

- スタンドアロン モード – 最大 8 つのスイッチを 1 つのファイアウォールに個別のポートを経由して相互接続できます。
- デイジーチェーン モード – 最大 8 つのスイッチを 1 レベルのチェーンの複数の構成でサポートできます。例を以下に示します。
    - 4 つのスイッチをスタンドアロン モードで接続し、1 つのスイッチをデイジーチェーン モードで相互接続する。

- 6 つのスイッチをスタンドアロン モードで接続し、さらに 2 つのスイッチを任意の 2 つにデイジーチェーン モードで個別に接続する。
- 7 つのスイッチをスタンドアロン モードで接続し、1 つのスイッチをそのいずれかにデイジーチェーン モードで接続する。

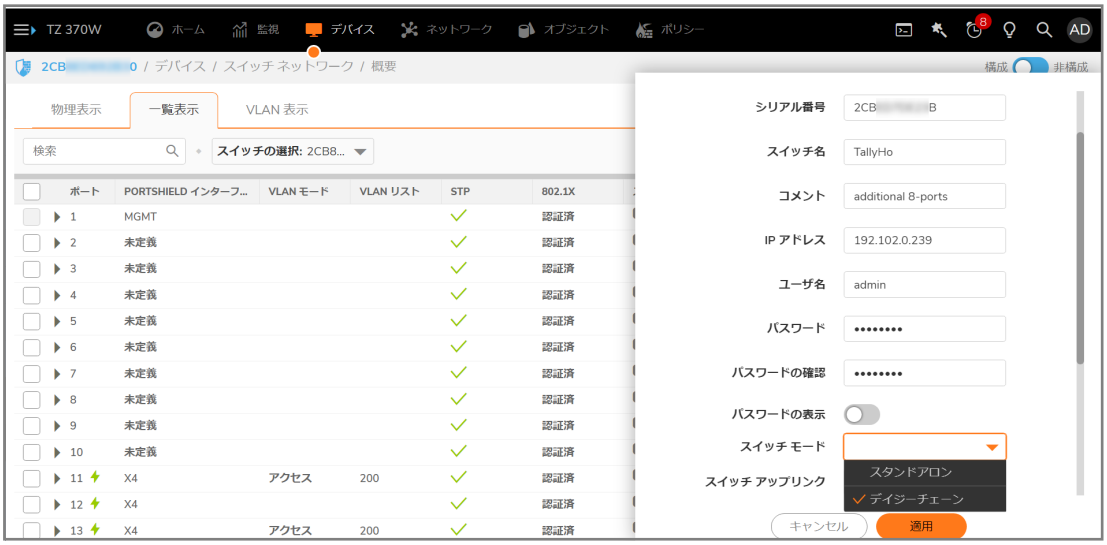
ⓘ **補足:** スイッチは、手動またはゼロタッチでデイジーチェーン構成に追加できます。

ⓘ **補足:** ファイアウォールと親スイッチ間に未構成の接続を追加すると、親スイッチと子スイッチ間のリンクは停止します。この問題を回避するには、物理的接続を行う前に、ファイアウォールと親スイッチ間で追加リンクを構成してください。

子スイッチを親スイッチに接続したら、「**デバイス | スイッチ ネットワーク > 概要**」ページにスイッチが表示されます。「**許可**」オプションをクリックするだけで、スイッチはデイジーチェーン モードで追加されます。

デイジーチェーン モードでスイッチを追加するには、以下の手順に従います

1. スタンドアロン構成のスイッチを選択し、追加のスイッチをそれにデイジーチェーン モードで接続します。次に、追加のスイッチの接続に使用するポートを決定します。
2. 「**デバイス | スイッチ ネットワーク > 概要**」に移動し、「**スイッチの追加**」をクリックします。



3. 「スイッチの追加」ダイアログ ボックスが表示されたら、下の説明に従って登録を行います。
   - IP アドレス – 親スイッチ用 DHCP サーバのリース内アドレスです。このアドレス範囲を識別するには、「**ネットワーク > DHCP サーバ**」に移動します。
   - スイッチ モード – 「デイジーチェーン」を選択します。
   - 親スイッチ ID – 最初にファイアウォールに追加されたスイッチに子スイッチが接続されている場合、スイッチ ID は 1 になります。
   - 親スイッチ アップリンク – 子スイッチに接続されている親スイッチのインターフェース。
   - スイッチ アップリンク – デイジーチェーン構成のスイッチが親スイッチに接続する際に利用するポート。
4. ダイアログ ボックスでの設定が完了したら、「**追加**」をクリックします。

   ⓘ **補足:** ファイアウォールに接続された最初のスイッチをスタンドアロンとして定義します。そのスイッチに接続されたスイッチをデイジーチェーンとしてセットアップします。
5. 「**デバイス | スイッチ ネットワーク > スイッチ**」に移動し、「**物理表示**」をクリックします。新しいスイッチが、スイッチとファイアウォールをリンクしているポートと共にグラフィックで表示されます。

アクセス ポイントをスイッチに接続

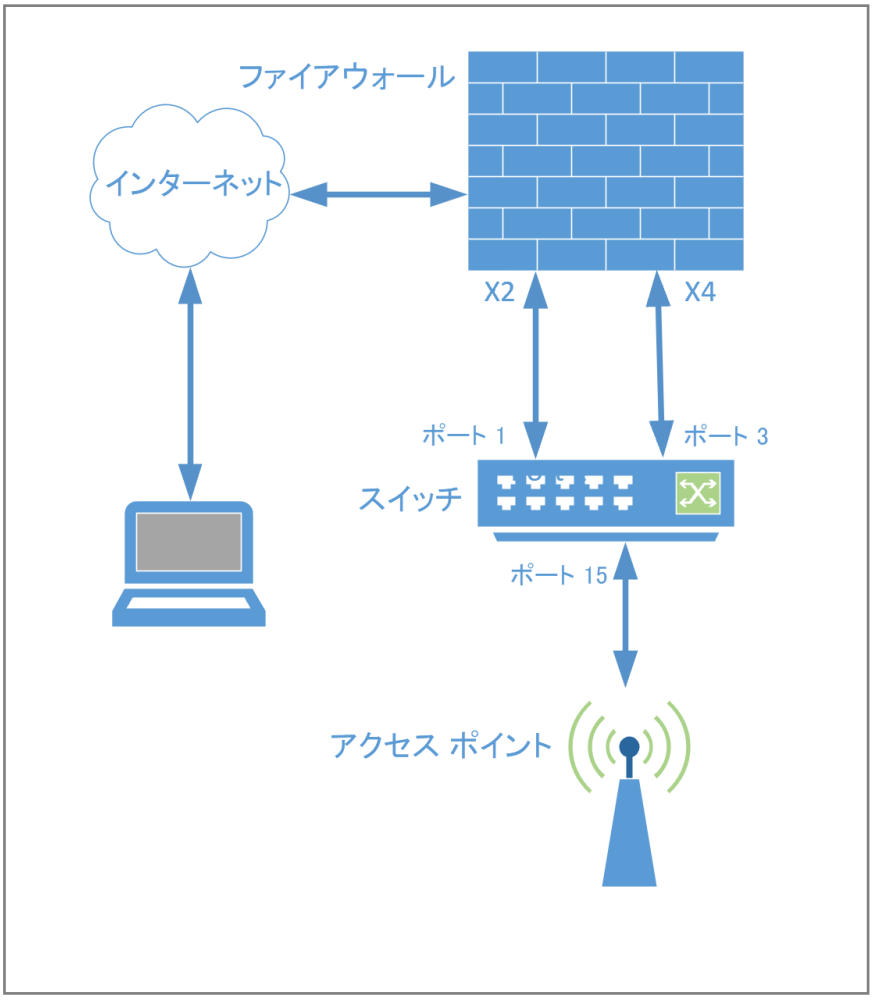
管理者は、ファイアウォール インターフェースを使用して、スイッチに接続された SonicWave アクセス ポイントを管理できます。アクセス ポイントをスイッチに追加する手順には、物理的な接続以外にも 3 つのステップが必要です。

- WLAN をサポートするように、アクセス ポイントをサポートしているスイッチに対してネットワーク インターフェースを構成します。
- 信頼できるセキュリティ サービスに関する WLAN ゾーンの構成を行います。
- SonicWave アクセス ポイントのエントリに対して適切な無線周波数、モード、認証種別の構成を行います。

以下は、ファイアウォール ― スイッチ ― アクセス ポイントの構成を図示したものです。

スイッチを介してアクセス ポイントを管理するには、以下の手順に従います

(この手順は以下の図を参考にしています)



1. スイッチのポート 1 を X2 インターフェースに接続し、X2 インターフェースで自動検出を有効にします。詳細については、「ゼロタッチによるファイアウォールへのスイッチ追加」を参照してください。
2. スイッチを追加します。

3. VLAN を使用して WLAN ゾーン内の X4 を構成します。
4. スイッチ ポート 3 を X4 インターフェースに接続します。
5. ファイアウォール GUI で、「**デバイス | スイッチ ネットワーク > スイッチ**」に移動し、「**一覧表示**」をクリックします。鉛筆アイコンをクリックしてポート 3 を構成します。詳細なアップリンクを作成するには、Portshield インターフェースを X4 に設定し、専用アップリンク スイッチを右へ移動します。
6. SonicWave アクセス ポイントをスイッチのポート 15 に接続します。
7. ポート 15 の「スイッチ ポート設定」にアクセスし、Portshield インターフェースを X4 に設定します。

   ポートを WLAN ゾーン内にある X4 インターフェースの任意の VLAN に設定する場合は、「VLAN の追加」を参照してください。
8. インターフェースに接続して Port-Shield が完了し、SonicWave がファイアウォール インターフェースに接続されたら、Sonicwave が構成されたネットワークから IP アドレスを取得することを確認します。

   確認の手順は、ファイアウォール GUI で、「**アクセス ポイント > 設定**」に移動し、「SonicWave オブジェクト」を選択します。

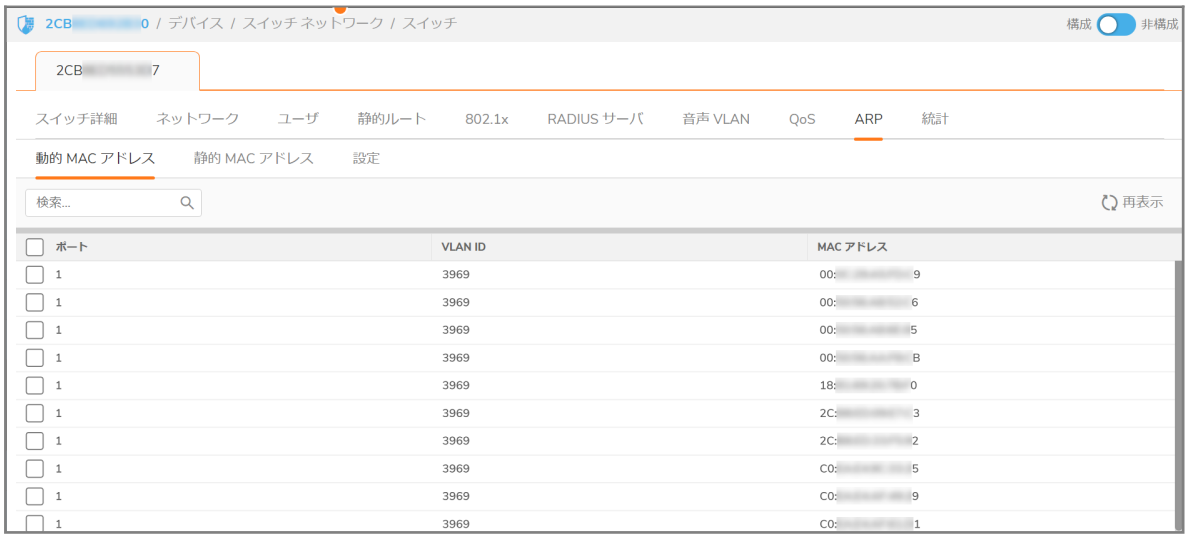
   SonicWave オブジェクトの設定に関する詳細は、「SonicWall アクセス ポイントへのリンクの設定」を参照してください。
9. WiFi クライアントを接続し、そのクライアントが X4 Portshield リースホールドから IP アドレスを取得することを確認します。

MAC アドレス テーブルの変 更

MAC アドレス テーブルは、受信イーサネット フレームで MAC 送信先アドレスを、前のフレームの送信から学習した内容に基づいて送信先に最も近いポートにリンクさせます。この機能を使用すると、以下のことができます。

- MAC エージング タイムの定義
- 静的 MAC テーブル エントリの設定
- 動的 MAC エントリ学習の確認

「**デバイス > スイッチ ネットワーク > スイッチ**」に移動し、「**ARP**」をクリックします。



MAC エージング タイムを設定するには、以下の手順に従います

MAC エージング タイムは、エントリから時間が経過して MAC アドレス テーブルから破棄されるまでの時間を指定します。範囲は 0 ～ 630 で、既定値は 300 秒です。MAC エージングの無効化はサポートされていません。このエージ指定はすべての VLAN に適用されます。

静的 MAC アドレスを追加するには、以下の手順に従います

1. 「静的 MAC アドレスの追加」をクリックすると、次のダイアログ ボックスが表示されます。

2. ポートおよび VLAN ID、それに送信先 MAC アドレスを選択して、「OK」をクリックします。

動的 MAC アドレス学習を確認するには、以下の手順に従います

動的 MAC アドレス テーブルには、現在学習中の MAC アドレスとそれに付属するポートおよび VLAN ID の一覧が表示されます。定義した MAC エージング タイムは、この情報がどれくらい新しいかを決定します。このテーブルには、スイッチによってサポートされる LAN に関する詳細が表示されます。

ポート統計の確認

「**デバイス | スイッチ ネットワーク > スイッチ > 統計**」の順に選択すると、スイッチの統計表も開きます。

この表には、ポート別のパフォーマンスの詳細が表示されます。

3

スイッチトポロジの設定

トピック:

基本トポロジの設定

トポロジについて

SWS12 または SWS14 シリーズ スイッチの基本トポロジの内容:

- 共通アップリンクを設定する
- 専用アップリンクを設定する
- 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 システムの設定
- 管理 / データ用のアップリンクとして隔離されたリンクを設定する
- 高可用性の設定
- アップリンクの設定
- SonicWall アクセス ポイントへのリンクの設定

リンクの概要

共通リンクは、データ トラフィックと管理トラフィックを伝送します。共通リンクは、すべての PortShield トラフィックとすべての PortShield 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します。このグループは、SonicWall ファイアウォール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。

隔離されたリンクは、管理トラフィックまたはデータ トラフィックを伝送します。両方を同時に伝送することはできません。一般に、隔離されたリンクは、ファイアウォールとスイッチを結ぶ複数の接続を使い、管理トラフィックとデータ トラフィックを別々に伝送します。

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。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のオプションを使うと、ファイアウォール アップリンクとして構成されたファイアウォールのポートと、スイッチ アップリンクとして構成された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。

補足: IDV — Interface Disambiguation via VLAN – スイッチ上で、ファイアウォール インターフェースに対してポートシールドしてポートを再設定し、PortShield VLAN に対応する VLAN アクセス ポートとします。

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、ファイアウォールとスイッチを接続する必要があります。
- インターフェースを PortShield ホストにすること（他のファイアウォール 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（他のファイアウォール 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。
- アップリンク インターフェースのスイッチ側は、子を持つことができません（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）。ファイアウォール アップリンク インターフェースは、子/サブ インターフェースを持つことができます。

スイッチ管理ポートをファイアウォールに接続する

スイッチの管理ポートに接続されたインターフェースの IP アドレスは、スイッチと同じサブネットにある必要があります。例えば、スイッチとファイアウォールの管理接続が X 2 を使う場合、X2 の IP アドレスは同じサブネット（192.168.168.10 など）に含まれる必要があります。既定スイッチの IP アドレスは 192.168.168.169 です。

スイッチ管理ポートおよびスイッチ アップリンク ポートとして指定されたスイッチ ポートでは、すべてのポートベースの設定操作が無効になっています。この設定により、これらの重要なポートで行われた設定操作がスイッチ到達可能性の問題を招き、この統合ソリューションを損なう危険性が排除されます。

共通アップリンクを設定する

SonicWall スイッチをファイアウォールによって管理することで、統合管理オプションを提供できます。共通アップリンク設定を使用すると、ファイアウォールとスイッチを結ぶ 1 本のリンクをすべての PortShield トラフィック（管理とデータの両方）を伝送するアップリンクとして指定できます。ファイアウォールのポートとスイッチのポートは、すべてのファイアウォール インターフェースに対応する VLAN のタグ付けされたトラフィックを伝送するためのトランク ポートとして構成されます。トラフィックの VLAN タグは、IDV（Interface Disambiguation via VLAN）のアプリケーションを利用して、トラフィックをそれが属する PortShield グループに適切に関連付けるために使用されます。

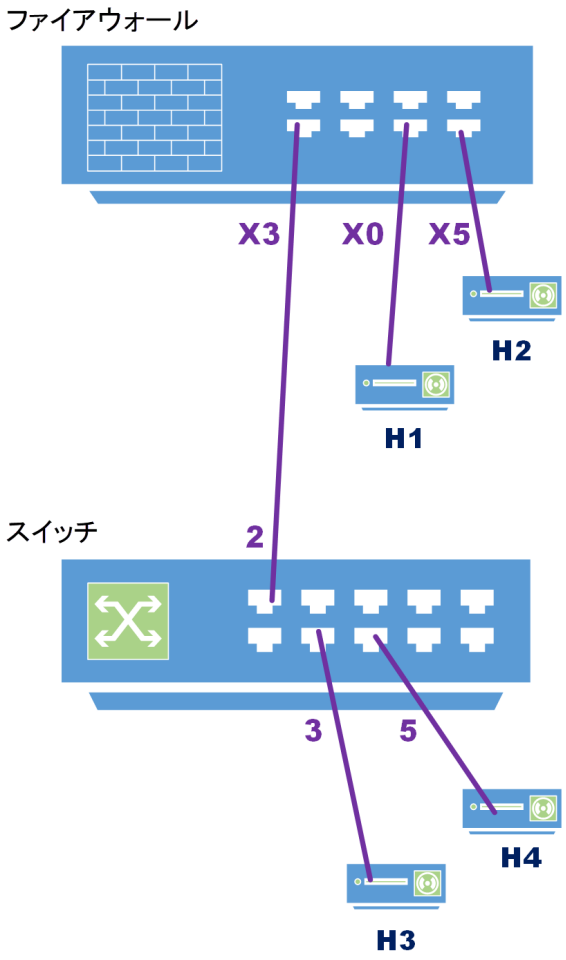
このような配備オプションのメリットは、管理トラフィックに使用していないファイアウォール/スイッチ ポートの一部を分離できることです。逆にデメリットは、データ トラフィックの量が多い場合、データ トラフィックと管理トラフィックが同じリンクを共有するため、管理トラフィックの転送が圧迫されることです。

「共通アップリンク トポロジ」の図は、1 つのファイアウォールと 1 つの SonicWall スイッチから構成される一般的な統合トポロジを示しています。

- ファイアウォール アップリンク インターフェースは X3 です。
- スイッチ アップリンク インターフェースは 2 です。

ファイアウォールの X3 とスイッチのポート 2 を結ぶこのアップリンクは、H1/H2 および H3/H4 の間で PortShield トラフィックを伝送するために設定された共通リンクです。また、このアップリンクは、ファイアウォールによるスイッチ管理に使用されるリンクでもあります。この構成では、X3 はスイッチの IP アドレスと同じサブネットで構成されます（「スイッチ管理ポートをファイアウォールに接続する」を参照してください）。また、X3 はファイアウォール アップリンクとして構成されます。

共通アップリンクのトポロジ



共通リンクを構成するには、以下の手順に従います

ファイアウォールとスイッチを結ぶ 1 本の共通リンクは、ゼロタッチによりスイッチを追加するか、手動で設定することで確立できます。詳細は下記を参照してください。

- スイッチ追加前
- ゼロタッチによるファイアウォールへのスイッチ追加
- 手動によるファイアウォールへのスイッチ追加

どちらのオプションを使用しても、適切なインターフェースを選択することで共通リンクを構成できます。

いずれの場合も、管理リンクを作成するには、スイッチ管理インターフェースの既定 IP アドレスを含む IP サブネットを解決するために、ファイアウォールの DHCP を構成する必要があります。詳細については、「スイッチ管理ポートをファイアウォールに接続する」を参照してください。

1. スイッチ管理ポートと同じ IP サブネットを使用して、ファイアウォール ポート X3 をセットアップします。
    a. 「**ネットワーク > DHCP サーバ**」に移動し、X3 インターフェースの構成アイコン（鉛筆）をクリックします。

b. スイッチ管理 IP アドレスを対象にするために、DHCP リースを構成します。スイッチ管理インターフェース用既定の IP アドレスは 192.168.168.169 であるため、DHCP スコープ設定の範囲にはこのアドレスを含める必要があります。

2. スイッチをネットワークに追加するには、「手動によるファイアウォールへのスイッチ追加」の説明に従い、「**デバイス | スイッチ ネットワーク > 概要 > 一覧表示**」に移動します。
   a. 「**スイッチの追加**」をクリックします。
   b. ダイアログ ボックスが表示されたら、「**スイッチ アップリンク**」および「**スイッチ管理**」ポートを 2 に設定し、「**ファイアウォール アップリンク**」を X3 に設定します。
   c. 「**適用**」をクリックして、設定を保存します。
3. 「**概要 > 物理表示**」で、ファイアウォールとスイッチ間の 1 本のリンクが表示されるはずです。

専用アップリンクを設定する

この設定を使うと、ファイアウォールとスイッチを結ぶ 1 本のリンクを、接続先のファイアウォール インターフェースに対応する PortShield トラフィックを伝送する専用アップリンクとして指定できます。ファイアウォールのポートとスイッチのポートは、ファイアウォール インターフェースの PortShield VLAN に対応する VLAN トランク モードに構成されます。

この設定は、専用 1G リンクが特定のファイアウォール インターフェースに必要とされる構成で使用できます。この設定が必要となる導入ケース:

- VLAN が使用される。例えば、スイッチの裏に別のスイッチがある場合など。
- トラフィックが非常に多く、このトラフィックのために別個のアップリンクが必要とされる。

このような構成の欠点は、ファイアウォール上のインターフェースが早くに使い果たされてしまうことです。

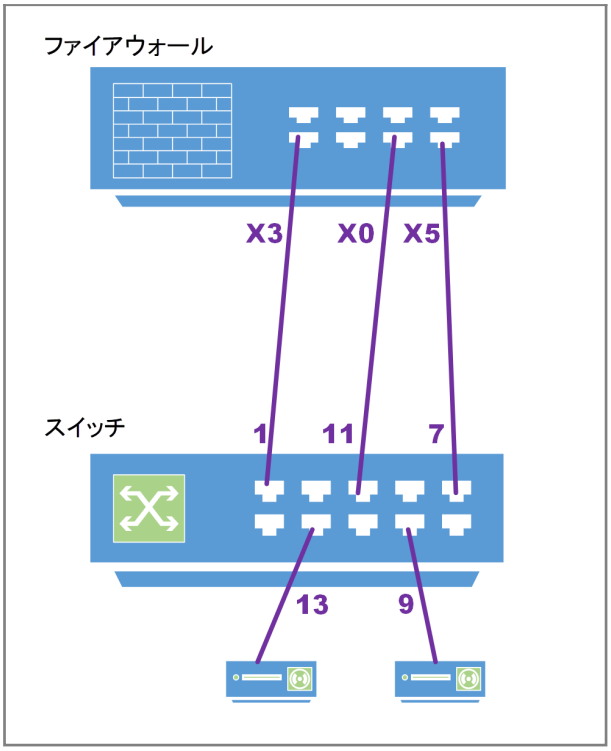
ⓘ | **補足:** この例では、ファイアウォール インターフェースの残りの部分 (専用リンクがある X0 と X5 を除く) に PortShield トラフィックを伝送する共通アップリンクはありません。

ⓘ | **重要:** 専用アップリンクが機能するには、構成を行う前に物理リンクを接続する必要があります。

専用アップリンク トポロジの図は、1 つのファイアウォールと 1 つのスイッチから構成される専用アップリンク セットアップを示しています。このシナリオでは、専用アップリンクが 2 つあります。

- ファイアウォールの X3 と SonicWall スイッチのポート 1 を結ぶアップリンクは、スイッチの管理に使用されます。この構成では、X3 がスイッチの IP アドレスと同じサブネットで構成されます。
- また、専用アップリンクが 2 つあります。
  - ファイアウォールの X0 とスイッチのポート 11 を結ぶリンクは、X0 のすべての PortShield トラフィックを伝送する専用リンクです。
  - ファイアウォールの X5 とスイッチのポート 7 を結ぶリンクは、X5 のすべての PortShield トラフィックを伝送する専用リンクです。

専用アップリンクのトポロジ



共通アップリンクを設定してもしなくても、複数のファイアウォール インターフェースのすべての PortShield トラフィックを伝送するために専用アップリンクを構成できます。両方のケースで、共通アップリンクがスイッチの管理に使用されます。

共通アップリンクなしで専用アップリンクトポロジを構成するには、以下の手順に従います

1. 「手動によるファイアウォールへのスイッチ追加」に従って、スイッチを設定します。
2. 管理トラフィックなしに専用アップリンクとしてリンクをセットアップするには、「スイッチの追加」ダイアログボックスで、「**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**」を「**なし**」に設定します。
3. 「**デバイス | スイッチ ネットワーク > 概要 > 物理表示**」または「**一覧表示**」で、専用リンク用のスイッチ ポートを有効にします。
4. スイッチ ポートが有効になったら、「ポートの設定」専用アップリンクをサポートするように Portshield を設定します。この例では、ポート 7 は X5 に対してポートシールドされます。

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 システムの設定

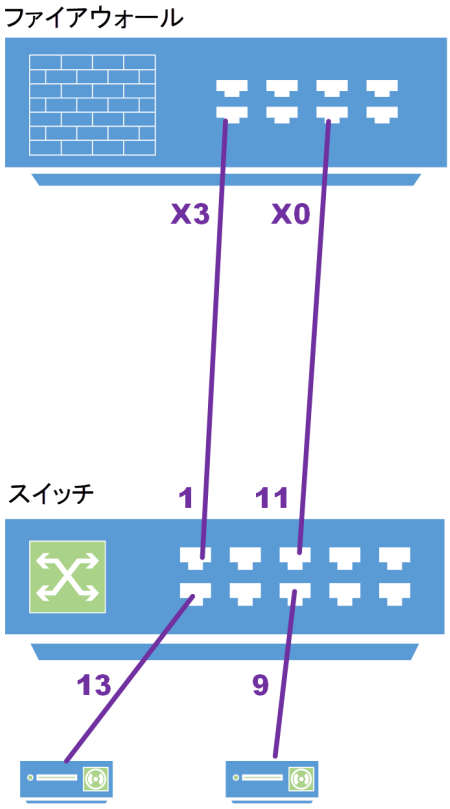
この設定では、共通アップリンクと専用アップリンクを組み合わせて、ファイアウォールとスイッチの間にセットアップすることができます。専用アップリンクは、接続先のファイアウォール インターフェースに対応する PortShield トラフィックを伝送するために使用されます。共通アップリンクは、残りのファイアウォール インターフェース（専用アップリンクが設定されていないもの）の PortShield トラフィックを伝送します。

ハイブリッド リンクのトポロジは、SonicWall ファイアウォールと SonicWall スイッチを使用するハイブリッド アップリンク統合トポロジを示しています。

- ファイアウォールの X0 とスイッチのポート 11 を結ぶ専用アップリンクは、X0 の PortShield トラフィックを伝送するためにセットアップされています。
- ファイアウォールの X3 とスイッチのポート 1 を結ぶ共通リンクは、X0 以外のファイアウォール インターフェースの PortShield トラフィックを伝送します。
- 専用アップリンクで結ばれるポート X0 と 11 は、X0 に対応する VLAN のトランク モード ポートです。共通アップリンクのポート X3 と 1 はトランク ポートで、X0 を除くすべてのファイアウォール インターフェースに対応する VLAN はメンバーとしてこのトランクに追加され、PortShield VLAN タグ付きトラフィックの伝送を容易にします。

この設定では、X3 と 1 を結ぶリンクがファイアウォールとスイッチの間で管理トラフィックを伝送するためにも使用されます。

ハイブリッド リンクのトポロジ



ハイブリッド設定をセットアップする手順は、次の 2 つです。

1. 共通アップリンクを構成します。
2. 専用アップリンクを構成します。

共通アップリンクと専用アップリンクを使用してハイブリッド設定をセットアップするには、以下の手順に従います

1. 「手動によるファイアウォールへのスイッチ追加」の説明に従って、スイッチを設定します。
2. 「専用アップリンクを設定する」の説明に従って、アップリンクを設定します。

管理 / データ用のアップリンクとして隔離されたリンクを設定する

この設定では、管理トラフィックとデータトラフィックを伝送するために、ファイアウォールとスイッチ間で個別のリンクを使用できます。共通リンクを使用すると、管理トラフィックとデータトラフィックは同じアップリンクで実行されます。データトラフィックが輻輳すると、管理トラフィックも密集するため、管理トラフィックの転送遅延が生じます。データトラフィックが輻輳する場合、管理トラフィックとデータトラフィックを別々のリンクで伝送することを検討してください。共通リンクの設定と似ていますが、管理とデータを隔離するこの設定では、管理トラフィックとデータトラフィックに別々のアップリンクを使用します。この設定を使うと、データトラフィックが多い時間帯でも管理トラフィックは遅延なしでスイッチに転送されます。

ⓘ | **重要:** 管理ポートは PortShield できません。

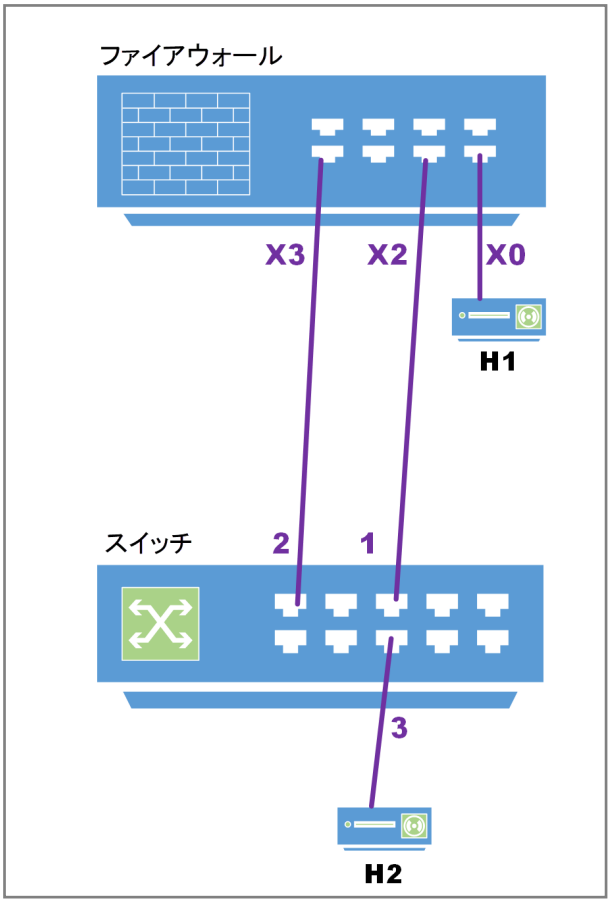
隔離されたリンクのトポロジは、1 つのファイアウォールと 1 つのスイッチの隔離されたリンク セットアップを示しています。

- ファイアウォールの X2 とスイッチのポート 1 を結ぶリンクは、管理トラフィックをスイッチに伝送します。この構成では、X2 が SonicWall スイッチの IP アドレスと同じサブネットで構成されます。

  ⓘ | **補足:** スイッチが隔離されたアップリンクを使用して構成される場合、スイッチ IP を静的 IP アドレスで構成する必要があります。
- ファイアウォールの X3 とスイッチのポート 2 を結ぶこのリンクは、管理トラフィックを除くすべてのデータトラフィックを伝送するためにセットアップされたアップリンクです。
- スイッチ インターフェースは X3 に対して直接 PortShield できませんが、X3 の VLAN インターフェースに対してはポートシールドできます。
- ポート 1 はスイッチ管理ポートとして構成されています。
- スイッチのポート 2 はデータ アップリンクとして機能します。
- スイッチのポート 3 は、X3 の VLAN インターフェースのいずれかに対して PortShield できます。

  ⓘ | **重要:** ファイアウォールで予約済みの VLAN レンジに変更を加えるには、SonicWall スイッチを追加する前に行ってください。スイッチの接続後に予約済みの VLAN レンジを変更する場合、スイッチの接続を解除してから再追加する必要があります。

隔離されたリンクのトポロジ



管理トラフィックとデータトラフィックを伝送するために隔離されたリンクをセットアップするには

1. スイッチ ポート 1 を、スイッチの管理 IP アドレスと同じサブネット内で構成されたファイアウォールの X2 に接続します。
2. スイッチ ポート 2 をファイアウォールの X3 に接続します。
3. 「**デバイス | スイッチ ネットワーク > 概要 > 一覧表示**」に移動し、「**スイッチの追加**」ボタンをクリックします。
4. ダイアログ ボックスが表示されたら、必要なデータと以下の設定を入力します。
   - スイッチ管理 = 1
   - ファイアウォール アップリンク = X3
   - スイッチ アップリンク = 2
5. 設定が完了したら、「**追加**」をクリックします。

高可用性の設定

トピック:

- 共通アップリンクによる HA および PortShield 設定
- 専用アップリンクによる HA および PortShield 設定
- 1 つのスイッチ管理ポートを使用した HA 設定
- 2 つのスイッチ管理ポートを使用した HA 設定

専用アップリンクによる HA および PortShield 設定

重要: HA でスイッチを使用するには、最初に HA ペアを作成し、その次にスイッチを追加する必要があります。

補足: ゼロタッチでスイッチを HA ペアに追加することはできません。「手動によるファイアウォールへのスイッチ追加」を参照してください。

専用アップリンクを使って高可用性を構成する方法は 2 通りあります。

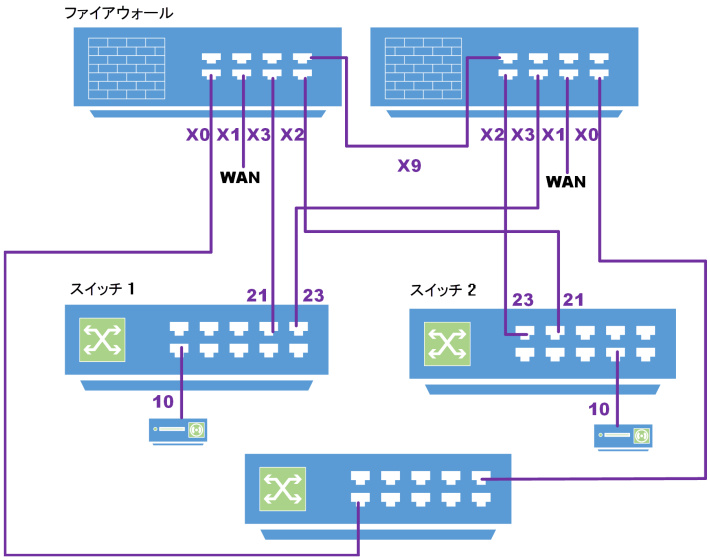
- 1 つのスイッチ管理ポートを使用した HA 設定
- 2 つのスイッチ管理ポートを使用した HA 設定

共通アップリンクによる HA および PortShield 設定

PortShield 機能を HA モードで使用するこの設定では、アクティブ/スタンバイ ファイアウォールとスイッチを結ぶリンクが、すべてのポートシールドされた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。PortShield ホストとして機能するファイアウォール インターフェースは、独立したスイッチ（スイッチでなくてもよい）に接続します。これは、アクティブ装置とスタンバイ装置に接続されたスイッチではありません。この別のスイッチは、同じ PortShield VLAN のパケットがループするのを回避します。PortShield メンバーは、アクティブ/スタンバイ ファイアウォールから制御されるスイッチのポートに接続できます。

共通スイッチを使用する HA ペアのトポロジは、1 つのファイアウォール ペアと 2 つのスイッチを示しています。X3 からスイッチ 1 間のリンクは、共通アップリンクとして設定されています。同様に、X2 からスイッチ 2 間のリンクも、共通アップリンクとして設定されています。PortShield ホストの X0 は、別のスイッチ（SonicWall スイッチでも他のベンダーのスイッチでもかまわない）に接続して、パケットのループを回避します。スイッチ 1 およびスイッチ 2 のポート 10 は、どちらも X0 に対してポートシールドされ、両方のスイッチでポート 10 に接続されたホストは共通アップリンクを使って通信できます。

共通スイッチを使用する HA ペアのトポロジ



共通アップリンクを使用して HA をセットアップするには、以下の手順に従います

ⓘ **補足:** HA ペアの作成後、手動でスイッチを追加します。スイッチの追加後に HA モードを有効にしても機能しません。

1. スイッチを追加して、データ アップリンクをセットアップします。
2. 「**ネットワーク > インターフェース**」ページで、両方のファイアウォールのインターフェースを次のように構成します。

X0	LAN/PortShield ホスト
X1	WAN
X2	スイッチ 2 用ファイアウォールにおけるファイアウォール アップリンク
X3	スイッチ 1 用ファイアウォールにおけるファイアウォール アップリンク

3. 以下のポートを除く共通アップリンクを構成します。

スイッチ 1 インターフェース	10	X0 に対してポートシールドされたホスト側インターフェース
	21	プライマリ ファイアウォールのスイッチ アップリンク
	23	セカンダリ ファイアウォールのスイッチ アップリンク
スイッチ 2 インターフェース	10	X0 に対してポートシールドされたホスト側インターフェース
	21	プライマリ ファイアウォールのスイッチ アップリンク
	23	セカンダリ ファイアウォールのスイッチ アップリンク

1 つのスイッチ管理ポートを使用した HA 設定

PortShield 機能を HA モードで使用するこの設定では、PortShield ホストとして機能するファイアウォール インターフェースが、アクティブ装置とスタンバイ装置でスイッチに接続する必要があります。PortShield メンバーも、スイッチのポートに接続する必要があります。PortShield ホストとして機能するファイアウォール インターフェースとスイッチを結ぶリンクは、専用アップリンクとしてセットアップされます。

1 つのスイッチ管理ポートを使用する HA ペアのトポロジは、1 つのスイッチおよび 1 つの専用リンクを含む 1 つのファイアウォール HA を示しています。

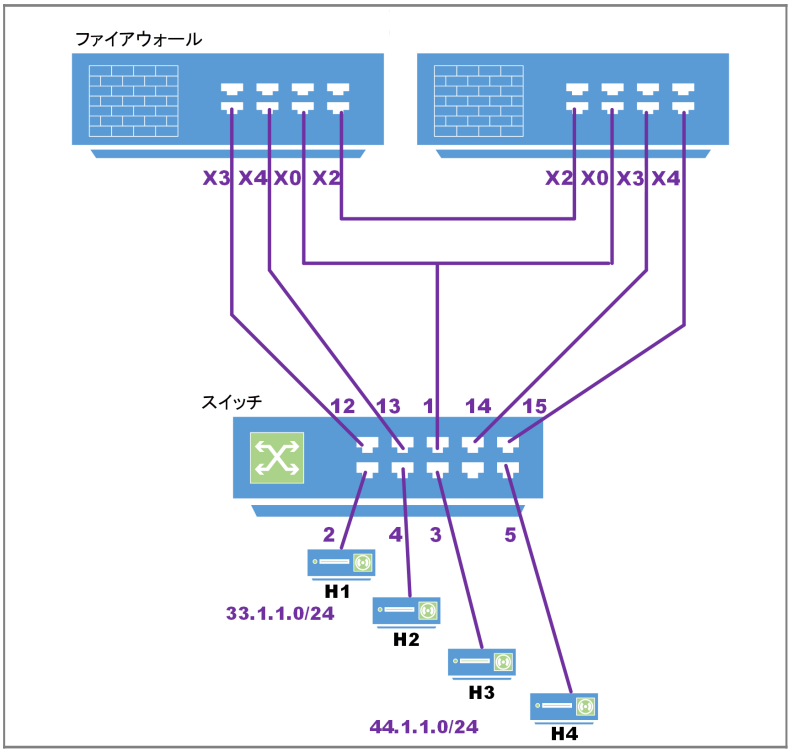
- プライマリ装置のファイアウォール インターフェース X3 と X4 は、スイッチのポート 12 と 13 に接続されます。
- X3 と X4 は、PortShield ホストとして構成されます。
- 同様に、セカンダリ装置のファイアウォール インターフェース X3 と X4 は、スイッチのポート 14 と 15 に接続されます。
- スイッチのポート 12 と 14 は、専用アップリンク オプションを有効にして X3 に対してポートシールドされます。
- スイッチのポート 13 と 15 は、専用アップリンク オプションを有効にして X4 に対してポートシールドされます。
- ポート 2 と 4 は、X3 に対してポートシールドされます。
- ポート 3 と 5 は、X4 に対してポートシールドされます。

プライマリ装置がアクティブな HA モードで動作すると、H1 と X3 の間のトラフィックは X3 と 12 を結ぶ専用リンクで伝送され、H3 と X4 の間のトラフィックは X4 と 13 を結ぶ専用リンクで伝送されます。

セカンダリ装置がアクティブな HA モードで動作すると、H1 と X3 の間のトラフィックは X3 と 14 を結ぶ専用リンクで伝送され、H3 と X4 の間のトラフィックは X4 と 13 を結ぶ専用リンクで伝送されます。

ファイアウォール インターフェース X0 とスイッチのポート 1 を結ぶリンクは、ファイアウォールからスイッチを管理するための管理トラフィックを伝送します。このような構成では、X0 がスイッチと同じサブネットに構成されます。また、セカンダリ ファイアウォールがアクティブな装置となったときにスイッチの管理がセカンダリ装置のファイアウォール インターフェース X0 とスイッチのポート 1 を結ぶリンクを介して行えるように、プライマリ装置とセカンダリ装置の X0 がスイッチのポート 1 に (例えばハブ経由で) 接続されている必要があります。このような構成では、スイッチのプロビジョニング時に、「プライマリ スイッチ管理」と「セカンダリ スイッチ管理」が 1 に設定されます。

1 つのスイッチ管理ポートを使用する HA ペアのトポロジ



1 つの専用アップリンクを使って HA をセットアップするには、以下の手順に従います

ⓘ **補足:** HA ペアの作成後、手動でスイッチの追加します。スイッチの追加後に HA モードを有効にしても機能しません。

1. スイッチを追加して、データ アップリンクをセットアップします。
2. 以下のオプションを構成します。

   ⓘ **補足:** 「ファイアウォール アップリンク」オプションと「スイッチ アップリンク」オプションは、冗長ファイアウォールをサポートするためにこの構成では同じ設定になります。

   a. それぞれのドロップダウン メニューから管理およびアップリンク インターフェースを選択し、「追加」をクリックします。
   b. プライマリおよびセカンダリ ファイアウォール両方の管理アップリンクを、スイッチ ポート 1 およびファイアウォール インターフェース X0 に設定します。

2 つのスイッチ管理ポートを使用した HA 設定

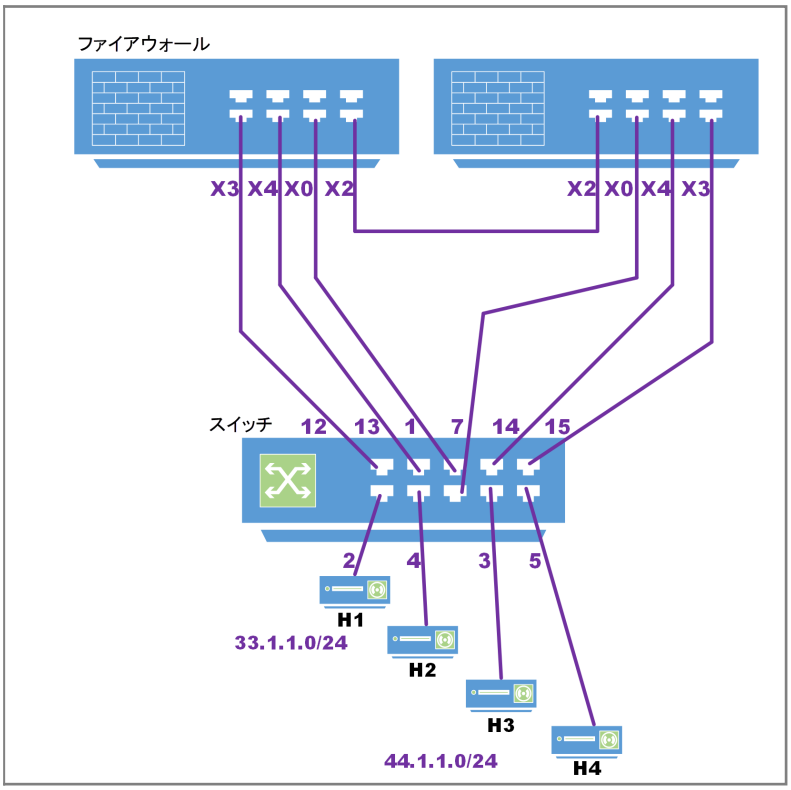
プライマリおよびセカンダリ ファイアウォールの X0 をスイッチのポートに直接接続することができます。この場合、スイッチの 2 つのポートが管理トラフィック用スイッチで使用されます。

2 つのスイッチ管理ポートを使用する HA ペアのトポロジは、1 つのスイッチおよび 2 つの専用リンクを含む 1 つのファイアウォール HA ペアを示しています。

- プライマリ装置の X0 はポート 1 に接続されます。
- セカンダリ装置の X0 はポート 7 に接続されます。

プライマリ ファイアウォールがアクティブな場合、プライマリの X0 とスイッチのポート 1 を結ぶリンクが管理トラフィックを伝送します。セカンダリ ファイアウォールがアクティブな場合、セカンダリの X0 とスイッチのポート 7 を結ぶリンクがファイアウォールによるスイッチ管理に使用されます。

2 つのスイッチ管理ポートを使用する HA ペアのトポロジ



2 つの拡張スイッチ管理ポートを使用して HA を設定するには、以下の手順に従います

ⓘ **重要:** HA ペアの作成後、手動でスイッチを追加します。スイッチの追加後に HA モードを有効にしても機能しません。

1. スイッチを追加して、データ アップリンクをセットアップします。
2. 以下のオプションを構成します。
   a. 2 つのスイッチ管理ポート構成の場合は、「**デバイス | スイッチ ネットワーク > 概要**」ページから「スイッチの追加」オプションを選択します。
   b. 「**ファイアウォールおよびスイッチ アップリンク**」オプションを「**なし**」に設定します。

   ⓘ **補足:** 一方を「プライマリ」、もう一方を「セカンダリ」として定義します。「ファイアウォール アップリンク」オプションと「スイッチ アップリンク」オプションは、HA モードで動作するファイアウォールには使用しません。プライマリ「ファイアウォール アップリンク」オプションとセカンダリ「スイッチ アップリンク」オプションは、「なし」に設定します。
3. 「**追加**」を選択します。

アップリンクの設定

トピック

- VLAN サポートの前提条件
- VLAN 向けの専用アップリンクを設定する

VLAN サポートの前提条件

- VLAN のサポートは、専用共通アップリンクで利用できます。例えば、専用アップリンクとして構成されたファイアウォール インターフェースに VLAN を構成できます。また、スイッチの共通アップリンクとしてプロビジョニングされるファイアウォール インターフェースにも VLAN を構成できます。
- 同じスイッチへの専用アップリンクとして構成された装置インターフェースに重複する VLAN は存在できません。VLAN 空間はスイッチ上でグローバルであるからです。例えば、X3 と X5 が同じスイッチの専用アップリンクとして構成されている場合、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。ただし、X3 と X5 が異なるスイッチへの専用アップリンクであれば、設定は受け入れられます。
- 重複する VLAN は、共通アップリンク インターフェースには存在できません。例えば、X3 があるスイッチへの共通アップリンクとして設定され、VLAN 100 が X3 に存在する場合、別のスイッチへの共通アップリンクとして構成された別のインターフェース、例えば X4 が VLAN 100 サブインターフェースを持つことはできません。
- アクセス/トランク設定用の VLAN を選択せずに、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。

ⓘ **重要:** ファイアウォールで予約済みの VLAN レンジに変更を加えるには、SonicWall スイッチを追加する前に行ってください。スイッチの接続後に予約済みの VLAN レンジを変更する場合、スイッチの接続を解除してから再追加する必要があります。

VLAN 向けの専用アップリンクを設定する

トピック

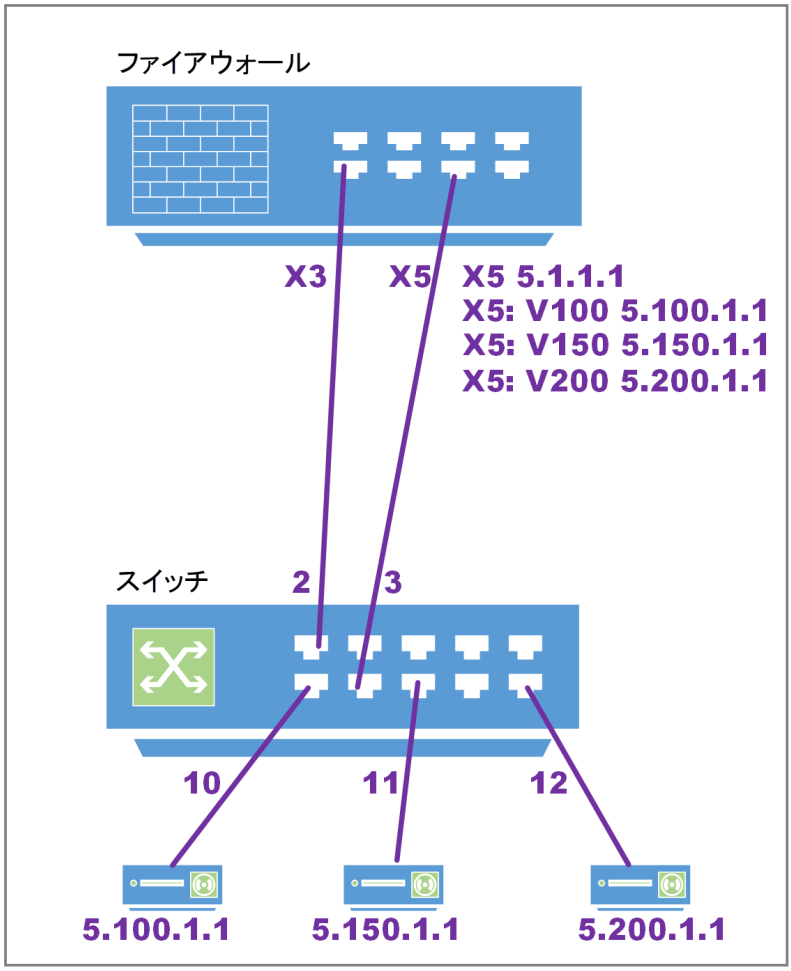
- VLAN 向けの専用アップリンクのトポロジ
- VLAN 向けの専用アップリンクを設定する

VLAN 向けの専用アップリンクのトポロジ

専用アップリンク構成では、ファイアウォールとスイッチを結ぶ特定のリンクが専用アップリンクとして指定され、このリンクが、ファイアウォール インターフェースに構成されたすべての VLAN のトラフィックと、ファイアウォール インターフェースに対応する PortShield トラフィックを伝送するようにセットアップされます。

ⓘ **補足:** VLAN は最初にファイアウォール インターフェースでセットアップする必要があります。

専用アップリンクを使用する VLAN のトポロジ



- X3 とスイッチのポート 2 を結ぶリンクは、ファイアウォールによるスイッチ管理に使用されます。
- インターフェース X3 は、スイッチの IP アドレスと同じサブネットに構成されます。

ⓘ **補足:** この例では、共通アップリンクが必要ないため、スイッチのプロビジョニングは、「ファイアウォール アップリンク」オプションと「スイッチ アップリンク」オプションを「なし」に、「スイッチ管理」を「1」に設定して実行します。

- 3 つの VLAN インターフェースが、VLAN タグ 100、150、および 200 で X5 に構成されています。
- ファイアウォールの X5 とスイッチのポート 3 を結ぶリンクは、X5 を経由する VLAN 100、150、および 200 でタグ付けされたトラフィックとタグ付けされないトラフィックを伝送するようにセットアップされた専用リンクです。

このトポロジをサポートするには、次のようにオプションを設定します。

- 専用アップリンク オプションを使って、ポート 3 を X5 に対してポートシールドします。
- ポート 10 を X 5 に対してポートシールドし、VLAN 100 を伝送するためにトランクとして構成します。
- ポート 11 を X 5 に対してポートシールドし、VLAN 150 を伝送するためにトランクとして構成します。
- ポート 12 を X 5 に対してポートシールドし、VLAN 200 を伝送するためにアクセスとして構成します。

VLAN 向けの専用アップリンクを設定する

VLAN サポートは、次の一連の手順に従うことで提供されます。

1. スイッチをプロビジョニングします。スイッチは、次の設定を行ってプロビジョニングできます。
   - VLAN サポートのみが必要な場合は、「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」を「なし」に設定します。
   - VLAN サポートに加え、他のファイアウォール インターフェースの PortShield トラフィックを伝送する共通トランク インターフェースのサポートも必要な場合は、共通アップリンク オプションを使用します。
2. 次の手順で専用リンクを構成します。
   a. ファイアウォール インターフェースに物理的に接続されたスイッチ ポートを選択します。
   b. ファイアウォール インターフェースに対してポートを PortShield します。
   c. 専用リンク オプションを選択します。
3. VLAN を有効にする必要があるスイッチ ポートを選択します。
4. ファイアウォール インターフェースに対してこのスイッチ ポートを PortShield します。
5. 「VLAN」タブで必要な VLAN を構成します。

共通アップリンクなしで VLAN 向けの専用アップリンクを構成するには、以下の手順に従います

詳細については、「専用アップリンクを設定する」を参照してください。

1. スイッチを追加して、「手動によるファイアウォールへのスイッチ追加」の説明に従いデータ アップリンクをセットアップします。
2. 「専用アップリンク」オプションを選択することを除き、「専用アップリンクを構成する」の説明に従いオプションを構成します。
3. 「**ネットワーク > インターフェース**」に移動します。
4. 「インターフェース設定」テーブルで、構成するインターフェースの構成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。
5. 「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。

   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。
6. 「**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。
7. 「**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。
8. 「OK」をクリックします。

この設定では、スイッチのポート 3 が VLAN 100、150、および 200 のタグ付きトラフィックと、IDV VLAN 6 のタグ付きでないトラフィックを伝送します。ポート 10 は VLAN 100 のタグ付きトラフィックを伝送するトランク ポートで、ポート 11 は VLAN 150 のタグ付きトラフィックを伝送するトランク ポートです。ポート 12 は VLAN 200 のタグ付きトラフィックを伝送するアクセス ポートです。ポート 10、11、および 12 は、X5 とポート 2T を結ぶ専用リンクを介して X5 に対してポートシールドされます。

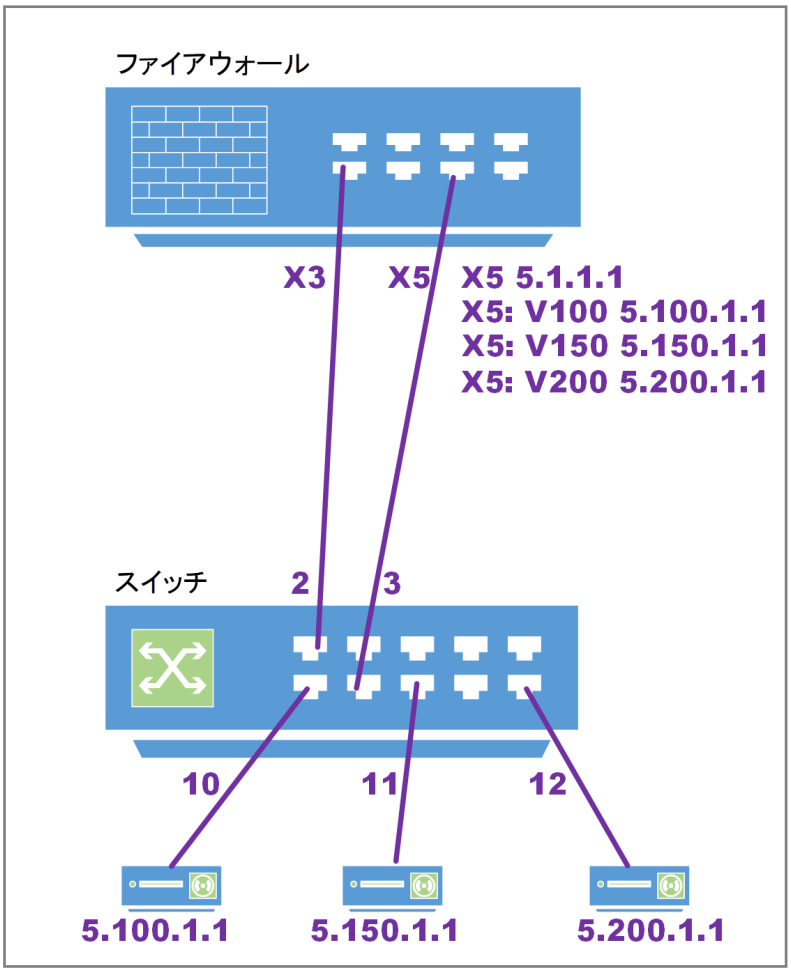
SonicWall アクセス ポイントへのリンクの設定

アクセス ポイントは複数の VLAN を伝送し、VLAN トンネルをパススルーするため、SonicWall アクセス ポイントを専用リンクを介して接続することを推奨します。専用リンクは、スイッチからファイアウォールまでタグ付きトラフィックをアクセス ポイントからパススルーするトランクとして機能します。

特定の管理がない非 SonicWall アクセス ポイントの場合、ファイアウォールのポートを「すべて」(LAN/WAN/DMZ、ただし一般には LAN) として構成できます。この場合、ファイアウォールとスイッチのポート ペアを専用リンクとして構成する必要があります。RJ45 でアクセス ポイントに接続する予定の他のスイッチ ポートは、この専用ポートに対してポートシールドされます。

SonicWall アクセス ポイントがファイアウォールの背後にあり、管理対象とする場合は、ファイアウォールとスイッチのペア ポートを専用リンクとして構成する必要があります。ファイアウォールの専用ポートは、WLAN として構成される必要があります。RJ45 で SonicWall アクセス ポイントに接続する予定の他のスイッチ ポートは、この専用ポートに対してポートシールドされます。

アクセス ポイントへの接続



SonicWall アクセス ポイント向けの専用アップリンクを構成するには、以下の手順に従います

1. 「管理 / データ用のアップリンクとして隔離されたリンクを設定する」の説明に従って、隔離されたリンクを使用してスイッチを追加します。
2. 「アクセス ポイントをスイッチに接続」の説明に従って、アクセス ポイントをスイッチに接続します。.
3. 「アップリンクの設定」の説明に従って、アップリンクを設定します。.
4. すべての SonicWall アクセス ポイントが、専用リンクの PortShield グループに構成されたスイッチ ポートに接続されていることを確認します。

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

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

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: 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 スイッチ ネットワーク 管理者ガイド
更新日 – 2021 年 4 月
ソフトウェア バージョン – 7
232-005451-10 Rev C

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次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、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035