SonicOS および SonicOSX 7

デバイス AppFlow

管理者ガイド

SONICWALL®

目次

1

フロー報告

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

ファイアウォールのフロー報告、統計、AppFlow およびリアルタイム データをローカル コレクターまたは外部 AppFlow サーバに送信するための構成可能な設定の管理には、AppFlow 機能を使用します。AppFlow は、NetFlow バージョン 5、NetFlow バージョン 9、IPFIX、拡張 IPFIX といった外部 AppFlow 報告形式をサポートします。AppFlow は Quest™ Change Auditor for SonicWall をサポートしています。これは、インターネット ウェブ サイトおよびクラウド アクティビティに関するデータを収集できる自動監査モジュールです。

「**デバイス | AppFlow > フロー報告**」ページには、フロー報告と内部報告に基づいて統計を表示するためにファイアウォールを構成する設定が含まれています。このページから、内部報告のほか、AppFlow エージェント、外部コレクターの報告、SonicFlow レポート (SFR) メーリングに関する設定を構成することもできます。

「AppFlow 報告」ページにアクセスするには、「**デバイス | AppFlow > フロー報告 | 設定**」ページで「**統合 AppFlow 報告データ コレクションを有効にする**」を有効にします。

「**デバイス | AppFlow > フロー報告**」の各タブの下部にある「**既定の設定**」ボタンをクリックすると、各ページの AppFlow 設定を消去して既定値に戻すことができます。

「**デバイス | AppFlow > フロー報告**」ページには、以下のタブがあります。

統計 – 報告統計を 4 つのテーブルで表示する

設定 – 各種のリアルタイム データ収集と AppFlow 報告収集を有効にできるようにする

AppFlow エージェント – AppFlow エージェントに報告する AppFlow を設定できるようにする

外部コレクター – IPFIX コレクターに報告する AppFlow を設定できるようにする

SFR メール設定 – SonicFlow レポート (SFR) を送信するためのメール サーバを設定できるようにする

トピック:

統計

この画面には、各種のフロー (サーバに送信された、収集されていない、破棄された、メモリに保存/削除された、サーバに報告された/報告されていない) に関するレポートが表示されます。また、このセクションには送信された NetFlow と IPFIX (IP Flow Information Export) テンプレートの数と、報告された一般静的フローが含まれます。

トピック:

外部フロー報告統計

統計	表示される総数
キューされた接続フロー:	これまでに収集された接続関連のフロー。
キューから出された接続フロー:	内部 AppFlow コレクターまたは外部コレクターのどちらかに報告された接続関連のフロー。
破棄された接続フロー:	報告に失敗した接続関連の収集されたフロー。
報告が省略された接続フロー:	報告が省略された接続関連のフロー。これは、収集されたフローが報告のために構成された値よりも多い場合に、定期モードの実行時に発生する可能性があります。
キューされた接続以外のデータ:	これまでに収集された接続関連以外のすべてのフロー。
キューから出された接続以外のデータ:	外部コレクターまたは内部 AppFlow コレクターのどちらかに報告された接続関連以外のすべてのフロー。
破棄された接続以外のデータ:	要求が多すぎて破棄された接続関連以外のすべてのデータ。
報告された接続関連以外の静的データ:	報告された接続関連以外の静的データ。これには、アプリケーション、ウイルス、スパイウェア、侵入、テーブル マップ、カラム マップ、ロケーション マップの一覧が含まれます。
IPFIX によるログ報告	IPFIX によって報告されたすべてのログ。

内部 AppFlow 報告統計

統計	表示される総数
キューされたデータ フロー:	AppFlow コレクターのキューに入れられた接続関連のフロー。
キューから出されたデータ フロー:	データベースに正しく挿入されたすべての接続関連のフロー。
破棄されたデータ フロー:	接続速度が速いためにデータベースへの挿入に失敗した接続関連のフロー。
報告が省略されたデータ フロー:	報告が省略された接続関連のフロー。
キューされた一般フロー:	データベース キュー内の接続関連以外のすべてのフロー。
キューから出された一般フロー:	データベースに正しく挿入された接続関連以外のすべてのフロー。
破棄された一般フロー:	速度が速いために（要求が多すぎて）データベースへの挿入に失敗した接続関連以外のすべてのフロー。
キューから出された一般静的フロー:	データベースに正しく挿入された接続関連以外のすべての静的フロー。
AppFlow コレクター エラー:	AppFlow データベース エラー。
データベース内のフロー総数:	データベース内の接続関連のフロー。

IPFIX 合計統計

IPFIX 統計は、「**統計**」画面の下部にある 2 つのテーブルに表示されます。

統計	表示される総数
送信された NetFlow/IPFIX パケット合計:	これまでに収集されたすべての/外部コレクター/AppFlow サーバ/AppFlow エージェントに送信された IPFIX/NetFlow パケット。
外部コレクターに送信された NetFlow/IPFIX パケット:	これまでに外部コレクターに送信された IPFIX/NetFlow パケット。
AppFlow エージェントに送信された NetFlow/IPFIX パケット	これまでにAppFlow サーバに送信された IPFIX/NetFlow パケット。
送信された Netflow/IPFIX テンプレート	すべての/外部コレクター/AppFlow サーバ/AppFlow エージェントに送信された IPFIX/NetFlow テンプレート。
外部コレクターに送信された接続フロー	外部コレクターに報告された接続/静的/一般フロー。
AppFlow サーバに送信された接続フロー	AppFlow エージェントに報告された接続/静的/一般フロー。
外部コレクターへの非接続関連動的:	これまでに外部コレクターに送信された IPFIX/NetFlow パケット。
AppFlow サーバへの接続関連以外の動的:	これまでにAppFlow サーバに送信された IPFIX/NetFlow パケット。
外部コレクターへの否接続関連静的:	AppFlow コレクター、または外部コレクターに報告された接続/静的/一般フロー。
IPFIX による外部コレクターへのログ報告	これまでに IPFIX によって外部コレクターに報告されたログ。
AppFlow サーバへの接続関連以外の静的:	AppFlow エージェントに報告された接続/静的/一般フロー。
IPFIX による AppFlow サーバへのログ報告	これまでに IPFIX によって AppFlow エージェントに報告されたログ。

設定

「**設定**」タブには、ローカル内部フロー報告、AppFlow サーバ外部フロー報告、および IPFIX コレクターに関する構成可能なオプションがあります。

トピック:

- 設定
- ローカル サーバ設定
- その他の報告設定

設定構成

「設定」画面の「設定」セクションでは、リアルタイム データ収集と AppFlow 報告収集を有効にできます。

- **接続報告** — 以下のモードのいずれかに従って AppFlow 報告収集を有効にします。
  - **すべて** — このチェックボックスをオンにすると、すべてのフローが報告されます。このオプションは既定の設定です。
  - **インターフェース基準** – このチェックボックスをオンにすると、発信または応答インターフェースのみを基準とするフロー報告が有効になります。これは、どのフローが外部または内部に報告されるかを制御する手段を提供します。有効にすると、フローは「**ネットワーク | インターフェース**」ページのインターフェース毎のフロー報告設定を検証します。
    インターフェースでフロー報告が無効になっている場合は、そのインターフェースに関連するフローは省略されます。
  - **ファイアウォール/アプリケーション ルール基準** – このチェックボックスをオンにすると、既存のファイアウォール アクセス ルールとアプリケーション ルールの設定 (それぞれ「**ポリシー | ルールとポリシー > アクセス ルール**」ページと「**ポリシー | ルールとポリシー > アプリケーション ルール**」ページに

存在）を基準とするフロー報告が有効になります。これはインターフェース基準の報告に似ています。唯一の違いはインターフェース毎の設定が確認されるのではなく、ファイアウォール毎のルールが選択されることです。

すべてのファイアウォール アクセス ルールとアプリケーション ルールには、フロー報告を有効にするためのチェックボックスがあります。このチェック ボックスを有効にすると、ルールに適合するフローが報告される場合に、ファイアウォール ルールにおけるフロー報告が有効かどうかが強制的に確認されます。

ⓘ **補足:** このオプションが有効でも、フロー報告オプションが有効になっているルールがなければ、データは報告されません。このオプションは、どのフローが報告される必要があるかを制御するための追加の手段です。

- **リアルタイム データ収集を有効にする** – ファイアウォール上でのリアルタイム データ収集を有効にしてリアルタイムの統計情報が得られるようにします。「**次のリアルタイム データを収集する**」ドロップダウン メニューで、個々の項目を有効/無効にできます。この設定はデフォルトで有効になっています。

  この設定が無効の場合、「**監視 | リアルタイム グラフ > システム監視**」ページに表示されるリアルタイム グラフが無効になるので、「システム監視」はストリーミング データの収集と表示を行いません。

  - **次のリアルタイム データを収集する** – 「**システム監視**」ページに表示するストリーミング グラフを選択します。既定では、すべての項目が選択されています。

オプション	表示するグラフ
上位アプリケーション	アプリケーション
毎秒のビット数	帯域幅
毎秒のパケット数	パケット速度
平均パケット サイズ	パケット サイズ
毎秒の接続数	接続速度と接続数
コア使用率	マルチコア監視
メモリ使用率	メモリ使用率

- **統合 AppFlow 報告データ コレクションを有効にする** – 有効にすると、ファイアウォールは統合報告用にデータ収集を開始します。各項目は次のセクションで有効/無効にできます。無効にすると、ダッシュボードの下の AppFlow 報告は無効になります。

  この設定が無効の場合、「AppFlow 報告」ではデータの収集と表示が行われません。

  ⓘ **ヒント:** 「**統合 AppFlow 報告データ コレクションを有効にする**」チェックボックスのそばにある**表示**アイコンを選択すると、「**調査 | 報告 | AppFlow 報告**」ページをすばやく表示できます。

  - **以下の報告データを収集する** – 個々の**報告データ コレクション**を有効/無効にします。このドロップダウン メニューから表示するデータを選択します。既定で、すべての報告が選択されています。

    - アプリケーション報告
    - ユーザ報告
    - IP 報告
    - 脅威報告
    - 地域 IP 報告
    - URL 報告

ローカル サーバ設定

「ローカル サーバ設定」セクションでは、内部コレクターに対する AppFlow 報告を有効にできます。

ローカル コレクターに AppFlow を送信する 内部サーバへの AppFlow 報告を有効にします。無効の場合、ダッシュボードの「AppFlow 監視」は無効です。

ⓘ **補足:** このオプションを有効/無効にするとき、この機能を完全に有効/無効にするために装置の再起動が必要になることがあります。

その他の報告設定

「その他の報告設定」セクションの各オプションは、接続を報告する条件を構成します。このセクションは接続関連以外のフローには適用されません。

- **破棄された接続を報告する** — 有効にすると、ファイアウォール ルールによって破棄された接続は報告されません。このオプションは既定で有効です。
- **スタック接続の報告を省略する** — 有効にすると、ファイアウォールの TCP/IP スタックによって始動または応答した接続は報告されません。既定で、このオプションは有効になっています。
- **以下の URL 種別を含める** — 報告が必要な URL の種別をドロップダウン メニューから選択します。特定の種別の URL 報告を省略するには、それらの種別を非選択 (無効) にします。

  ⓘ **補足:** この設定は、拡張 IPFIX を使っている場合 AppFlow (内部) と外部レポートの両方に適用されます。

Gif (既定で選択済み)	Json
Jpeg (既定で選択済み)	Css
Png (既定で選択済み)	Html (既定で選択済み)
Js	Aspx (既定で選択済み)
Xml	Cms

- **地域 IP 解決を有効にする** — 地域 IP 解決を有効にします。無効にすると、AppFlow 監視で「**始動者**」と「**応答者**」タブでの国に基づくフローのグループ化が行われなくなります。このオプションは、既定で非選択 (無効) になっています。

  地域 IP 遮断またはボットネット遮断を有効にすると、このオプションは無視されます。
- **IPv6 フローの報告を無効にする (すべて)** — IPv6 フローの報告を無効にします。この設定はデフォルトで有効になっています。

AppFlow エージェント

この画面では、AppFlow およびリアルタイム データを AppFlow エージェントに送信できます。AppFlow エージェントは、SonicWall Flow Analytics、GMS、または NSM です。

- **SonicWall AppFlow エージェントに AppFlow を送信する** – SonicWall 装置は、IPFIX を介して AppFlow データを SonicWall AppFlow エージェントに送信します。このオプションは既定では無効になっています。

  このオプションが無効になっていると、SonicWall AppFlow エージェントは、AppFlow 監視、AppFlow 報告、および AppFlow ダッシュボードのグラフを AppFlow エージェントに表示したり、リダイレクトにより別の SonicWall 装置に表示したりしません。

  ⓘ **補足:** このオプションを有効/無効にするとき、この機能を完全に有効/無効にするために装置の再起動が必要になることがあります。

- **SonicWall AppFlow エージェントにリアルタイム データを送信する** – SonicWall 装置は、IPFIX を介してリアルタイム データを SonicWall AppFlow エージェントに送信します。このオプションは、既定では無効になっています。

  このオプションが無効になっていると、SonicWall AppFlow エージェントは、リアルタイム グラフを AppFlow エージェントに表示したり、リダイレクトにより SonicWall 装置に表示したりしません。

- **SonicWall AppFlow エージェントにシステム ログを送信する** – SonicWall ファイアウォールは、IPFIX を介してシステム ログを SonicWall AppFlow エージェントに送信します。このオプションは、既定では選択されていません。

- **接続オープン時に報告する** – SonicWall 装置は新しい接続のオープンを報告します。接続がオープンした時点で対象の接続に関連するすべてのデータが利用可能であるとは限りません。このオプションにより、フローは新しい接続がオープンになって間もなく AppFlow エージェントに表示されます。このオプションは、既定では無効になっています。

- **接続クローズ時に報告する** – SonicWall 装置は新しい接続のクローズを報告します。これは、AppFlow エージェントに対してフローを報告するための最も効率的な方法です。対象の接続に関連するすべてのデータが利用可能で、報告されます。このオプションは既定で有効です。

- **AppFlow 報告形式** – 「**拡張 IPFIX**」または「**拡張 IPFIX v2**」を選択します。

- **以下の更新時に接続を報告する** – ファイアウォールは、指定された更新の発生を報告します。ドロップダウン メニューから更新を選択します。既定では、どの更新も選択されていません。

脅威検知	**VPN トンネル検知**
アプリケーション検知	**URL 検知**
ユーザ検知	

- **以下のテーブルに動的 AppFlow を送信する** – ファイアウォールは選択されているテーブルのデータを送信します。既定では、すべてのテーブルが選択されています。

接続	デバイス
ユーザ	スパム
URL	位置
URL 格付け	VOIP
VPN	

ⓘ **補足:** 拡張 IPFIX モードでは、選択されているテーブルについてファイアウォールが報告を生成できます。ファイアウォールは、このデータをキャッシュしていないので、送信されなかった一部のフローでは、他の関連データとフローを相関させる際にエラーが生成される場合があります。

外部コレクター

「**外部コレクター**」タブには、外部 IPFIX コレクターへの AppFlow 報告に関する設定があります。

- **フローとリアルタイム データを外部コレクターに送信する** – 指定したフローを外部フロー コレクターへ報告できるようにします。このオプションは、既定では無効になっています。

ⓘ **重要:** このオプションを有効/無効にするとき、この機能を完全に有効/無効にするために装置の再起動が必要になることがあります。

- **外部フロー報告形式** – 「外部フロー コレクターに対して報告する」オプションが選択されている場合、フロー報告の種別をドロップダウン メニューから選択する必要があります。

NetFlow バージョン 5 (既定値)	IPFIX
NetFlow バージョン 9	拡張 IPFIX

ⓘ **補足:** 「**外部フロー報告形式**」の選択内容に応じて、使用可能なオプションが変わります。

ⓘ **補足:** 拡張 IPFIX v2 は内部設定を有効することによってサポートされます。このオプションを有効にする方法については、SonicWall サポートにお問い合わせください。現在、AppFlow エージェントはこのバージョンの IPFIX をサポートしていません。

報告形式の設定により、以下のようになります。

- **Netflow** バージョン 5、9 または **IPFIX** に設定されている場合は、任意のサードパーティ製コレクターを使用して、ファイアウォールから報告されたフローを表示できます。ファイアウォールでは、IETF で定義されている標準データ形式を使用しています。**Netflow** バージョンおよび IPFIX 報告形式には、接続関連フローの詳細情報のみが標準に従って含まれています。
- **拡張 IPFIX** に設定されている場合、以下に関する SonicWall 動的テーブルの報告に SonicWall フロー対応のコレクターのみを使用できます。

接続	ユーザ	アプリケーション	ロケーション
URL	ログ	デバイス	VPN トンネル
デバイス	スパム	無線	
脅威（ウイルス/スパイウェア/侵入）	リアルタイム状況（メモリ/CPU/フェースの統計）		

このモードで報告されるフローは、コレクターとして構成された別の SonicWall ファイアウォール（特に、高可用性ペアでアイドル ファイアウォールがコレクターとして動作している場合）から、または SonicWall Linux コレクターから表示できます。標準 IPFIX サポートを使用しているいくつかのサードパーティ製コレクターも、このモードを使用してアプリケーションを表示できます。ただし、サードパーティ製コレクターですべての報告を表示できるわけではありません。

ⓘ **補足:** **拡張 IPFIX** を使う場合は、Scrutinizer など、SonicWall フローに対応したサードパーティ製コレクターを選択してください。

- **外部コレクターサーバ アドレス** – 装置が Netflow/IPFIX を通してフローを送信する外部コレクター IP アドレスを指定します。コレクターがフロー報告を生成するためには、この IP アドレスは SonicWall ファイアウォールから到達可能である必要があります。コレクターが VPN トンネル経由で到達可能な場合、「VPN トンネルでコレクターを使用する際の送信元 IP」に送信元 IP を指定する必要があります。
- **VPN トンネルでコレクターを使用する際の送信元 IP**– 外部コレクターに VPN トンネルを通して到達する必要がある場合、正しい VPN ポリシーに対する送信元 IP アドレスを指定します。

  ⓘ **補足:** VPN ポリシー内で指定したローカル ネットワークから送信元 IP を選択します。指定した場合、Netflow/IPFIX フロー パケットは常に VPN パスを通ります。
- **外部コレクター UDP ポート番号** – 送信する NetFlow/IPFIX パケットの UDP ポート番号を指定します。既定のポートは 2055 です。
- 定期的に IPFIX/Netflow テンプレートを送信する – 装置はテンプレート フローを定期的に送信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す。

  ⓘ **補足:** このオプションは、NetFlow バージョン 9、IPFIX、および拡張 IPFIX でのみ利用可能です。

  NetFlow バージョン 9 および IPFIX は、データを送信する前に外部コレクターに知らせる必要があるテンプレートを使います。IETF により、コレクターがデバイスとの同期を保つために、報告するデバイスはテンプレートを通常の間隔で送信できる必要があります。コレクターが定期的にテンプレートを必要としなければ、この機能は無効にしてかまいません。
- **定期的に静的 AppFlow を送信する** – 指定された静的 AppFlow テーブルに関する IPFIX レコードの 1 時間ごとの送信が有効になります。このオプションは、既定では無効になっています。

  ⓘ **補足:** このオプションは拡張 IPFIX でのみ利用可能です。SonicWall Scrutinizer をコレクターとして使用する場合は、このオプションが選択されている必要があります。
- **以下のテーブルに静的 AppFlow を送信する** –ドロップダウン メニューから、フローに対して生成する静的マッピング テーブルを選択します。静的テーブルの詳細については、「NetFlow テーブル」を参照してください。

アプリケーション（既定で選択済み）	**サービス**（既定で選択済み）

ウイルス（既定で選択済み）	**格付けマップ**（既定で選択済み）
スパイウェア（既定で選択済み）	**テーブル マップ**
侵入（既定で選択済み）	**カラム マップ**
ロケーション マップ	

拡張 IPFIX モードで動作している場合は、ファイアウォールはユーザ、VPN、アプリケーション、ウイルス、スパイウェアの情報を関連付けるために、複数の種別のデータを外部デバイスに報告します。データは静的と動的の両方です。静的テーブルは、ほとんど変更されないので一度だけ必要とされます。外部コレクターの能力によっては、すべての静的テーブルが必要というわけではありません。

拡張 IPFIX モードで、ファイアウォールは静的マッピング テーブルを非同期で生成することにより、外部コレクターと同期できます。この同期は外部コレクターがファイアウォールよりも遅れて初期化されたとき必要となります。

- **以下のテーブルに動的 AppFlow を送信する**－ドロップダウン メニューから、フローに対して生成する動的マッピング テーブルを選択します。動的テーブルの詳細については、「NetFlow テーブル」を参照してください。

  ⓘ **補足:** このオプションは**拡張 IPFIX** でのみ利用可能です。ファイアウォールは選択されているテーブルに関するレポートを生成します。ファイアウォールは、この情報をキャッシュしていないので、送信されなかった一部のフローでは、他の関連データとフローを相関させる際にエラーが生成される場合があります。

接続（既定で選択済み）	**デバイス**
ユーザ（既定で選択済み）	**スパム**
URL（既定で選択済み）	**位置**
URL 格付け（既定で選択される）	VoIP（既定で選択済み）
VPN（既定で選択済み）	

- **IPFIX に以下の追加報告を含む**－フローに生成される追加の IPFIX 報告を選択します。ドロップダウン メニューから値を選択します。既定では何も選択されていません。統計は 5 秒毎に報告されます。

  ⓘ **補足:** このオプションは拡張 IPFIX でのみ利用可能です。

  - システム ログ – インターフェース状態の変化、ファン障害、ユーザ認証、HA フェイルオーバーとフェイルバック、トンネルのネゴシエーション、設定変更などのシステム ログを生成します。システム ログには、通常はフロー（セッション/接続）関連以外のイベント（ファイアウォールを通るトラフィックに依存しないイベント）が記録されます。
  - **上位 10 アプリケーション** － 上位 10 アプリケーションを生成します。
  - **インターフェース状況** － インターフェース毎の統計（インターフェース名、インターフェース帯域幅使用率、MAC アドレス、リンク状況など）を生成します。
  - **コア使用率** – コア毎の使用率を生成します。
  - **メモリ使用率** － 利用可能なメモリ、使用中のメモリ、AppFlow コレクターで使用中のメモリの状況を生成します。

  どちらのモードで動作していても、SonicWall は接続とフローに関連しない、より多くのデータを報告できます。これらのテーブルはこのセクション（追加の報告）下にグループ化されます。外部コレクターの能力によっては、すべての追加テーブルが必要というわけではありません。このオプションでは、必要なテーブルを選択できます。

- **接続オープン時に報告する** – 新しい接続の確立時にフローを報告します。接続がオープンした時点で対象の接続に関連するすべてのデータが利用可能であるとは限りません。ただし、このオプションでは、新しい接続が確立して間もなく外部コレクター上にフローが表示されます。既定で、このオプションは有効になっています。
- **接続クローズ時に報告する** – 接続のクローズ時にフローを報告します。これは、外部コレクターに対してフローを報告するための最も効率的な方法です。対象の接続に関連するすべてのデータが利用可能で、報告されます。既定で、このオプションは有効になっています。
- **動作タイムアウト時に接続を報告する** – 動作タイムアウト セッション数に基づく接続を報告します。有効になっている場合、ファイアウォールはアクティブなタイムアウト周期ごとにアクティブな接続を報告します。既定で、このオプションは無効になっています。

  ⓘ **補足:** このオプションを選択すると、「キロバイト交換時に接続を報告する」オプションを同時に選択できなくなります。このオプションが既にオンになっている場合に「**キロバイト交換時に接続を報告する**」を選択しようとすると、以下のメッセージが表示されます。

  - **秒数** – 動作タイムアウトまでの秒数を設定します。アクティブなタイムアウトでは範囲を 1 から 999 秒の間で設定できます。既定の設定は 60 秒です。
- **キロバイト交換時に接続を報告する** – キロバイトで指定した一定のトラフィック量が転送されたタイミングに基づいてフローを報告します。この設定が有効になっている場合、ファイアウォールは、アクティブな接続上で指定バイト数の双方向データが転送されるたびにアクティブな接続を報告します。このオプションは、長時間動作していて監視が必要なフローに対して理想的です。このオプションは、既定では選択されていません。

  ⓘ **補足:** このオプションを選択すると、「**動作タイムアウト時に接続を報告する**」オプションを同時に選択できなくなります。このオプションが既にオンになっている場合に「**動作タイムアウト時に接続を報告する**」を選択しようとすると、以下のメッセージが表示されます。

  - **交換されたキロバイト** – 報告を行うために必要となる、接続上で転送されるデータの量をキロバイト単位で指定します。既定値は 100 キロバイトです。
  - **1 度だけ報告** – 「**キロバイト交換時に接続を報告する**」オプションが有効になっている場合、指定した量のデータが接続上で転送されるたびに同じフローが繰り返し報告されます。これにより、ロードされたシステムで大量の IPFIX パケットが生成されることがあります。このオプションを有効にすると、レポートは 1 度しか送信されません。このオプションは、既定では選択されています。
- **以下の更新時に接続を報告する** – ドロップダウン メニューから接続報告を有効にする対象を選択します (既定ではすべてが選択されています)。

選択項目	報告するフロー
脅威検知	脅威特有のフロー。ウイルス、侵入、またはスパイウェアが検知されると、フローは再度報告されます。
アプリケーション検知	アプリケーション特有のフロー。精密パケット検査の完了時に、SonicWall 装置は、フローが特定のアプリケーションの一部であるかどうかを検知できます。識別されると、フローは再度報告されます。
ユーザ検知	ユーザ特有のフロー。SonicWall 装置は、フローをログイン資格情報に基づいてユーザ基準の検知に関連付けます。識別されると、フローは再度報告されます。
VPN トンネル検知	VPN トンネルを通して送信されたフロー。VPN トンネル上で送信されたフローが識別されると、フローは再度報告されます。

- **動作** – 以下のボタンをクリックすると、テンプレートと静的フロー データを非同期で生成します。

- 「**すべてのテンプレートを生成する**」– このボタンをクリックすると、IPFIX サーバ上でテンプレートの構築が開始されます。この生成には最長で 2 分かかります。

  ⓘ **補足:** このオプションは、**NetFlow バージョン 9**、**IPFIX**、および**拡張 IPFIX** でのみ利用可能です。

- 「**静的 AppFlow データを生成する**」– このボタンをクリックすると、IPFIX サーバへの大量のフローの生成が開始されます。この生成には最長で 2 分かかります。

  ⓘ **補足:** このオプションは**拡張 IPFIX** でのみ利用可能です。

- **外部コレクターにログ設定を送信する** –「**登録をすべて送信**」をクリックすると、必要なログの設定のフィールドを外部コレクターに送信します。

  ⓘ **ヒント:** このオプションは、「外部フロー報告形式」として「**拡張 IPFIX**」を選択した場合にのみ表示されます。

  ⓘ **補足:**「**登録をすべて送信**」をクリックする前に、SonicOS と外部コレクター サーバの接続が完了していることを確認してください。
  以下の場合は、ボタンを再度選択して設定を同期します。
  SonicOS がアップグレードされてログ イベントが新たに追加された場合。
  SonicOS と外部サーバの接続がしばらく停止し、ログ設定が編集された可能性がある場合。

SFR メール設定

「**SFR メール設定**」タブを使用して、SonicFlow レポート (SFR) が電子メール アドレスに自動的に送信されるように設定します。

トピック:

- SFR 電子メール設定
- 電子メール送信のスケジュール

SFR 電子メール設定

SonicFlow レポート (SFR) を電子メール アドレスに自動的に送信するには、以下の手順に従います

1. 「**デバイス | Appflow > フロー報告**」に移動します。
2. 「**SFR メール設定**」タブをクリックします。
3. 「**電子メールでレポートを送信する**」を選択します。
4. 以下のオプションを入力します。
    - 「**SMTP サーバホスト名**」フィールドに電子メール サーバのアドレスを入力します。
    - 「**電子メール送信先**」フィールドに受信者の電子メール アドレスを入力します。
    - 「**送信元電子メール**」フィールドに送信者として使用する電子メール アドレスを入力します。
    - 「**SMTP ポート**」フィールドに SMTP ポート番号を入力します。既定値は 25 です。
    - 「**接続セキュリティ方式**」ドロップダウン メニューから電子メールのセキュリティ方式を選択します。
        - **なし** (既定)
        - SSL/TLS
        - STARTTLS
5. 電子メール サーバに SMTP 認証が必要な場合は、「**SMTP 認証を有効にする**」を選択して、
    - 「**SMTP ユーザ名**」フィールドにユーザ名を入力します。
    - 「**SMTP ユーザ パスワード**」フィールドにパスワードを入力します。
6. 電子メール サーバがメール送信前の POP 認証をサポートしている場合は、「**メール送信前の POP 認証を有効にする**」を選択して、
    - 「**POP サーバ アドレス**」フィールドに POP サーバのアドレスを入力します。
    - 「**POP ユーザ名**」フィールドにユーザ名を入力します。
    - 「**POP ユーザ パスワード**」フィールドにパスワードを入力します。
7. 「**適用**」を選択します。

電子メール設定をテストするには、以下の手順に従います

1. 「SFR 電子メール設定」に必要な値を入力します。
2. 「**電子メールのテスト**」を選択します。
   電子メール設定が正しい場合は、確認ダイアログ ボックスが表示されます。
   電子メール設定が誤っている場合は、警告ダイアログ ボックスが表示されます。
   電子メール設定を確認し、もう一度やり直してください。

電子メールによる SFR レポート送信のスケジュール設定

レポートを 1 回だけ送信するか、繰り返し送信するか、またはその両方で送信するかをスケジュール設定することができます。

レポートの配信スケジュールを構成できます

1. 「**デバイス | Appflow > フロー報告**」に移動します。
2. 「**SFR メール設定**」タブをクリックします。
3. 「**電子メールでレポートを送信する**」を選択します。
4. 「**電子メール送信のスケジュール**」セクションで、「**スケジュールの編集**」をクリックします。「**このスケジュールの編集**」ページが表示されます。

5. 「**スケジュール名**」フィールドに、レポートの名前を入力します。
6. レポートが送信される頻度を選択します。
   - **1 回** – レポートは指定した日時に 1 回だけ送信されます。
   - **繰り返し** – レポートは指定した曜日と時刻に繰り返し送信されます。
   - **混在** – レポートは 1 回送信され、また指定した曜日と時刻に繰り返し送信されます。

トピック:

- SFR の 1 回のみの配信のスケジュール設定
- SFR の繰り返し配信のスケジュール設定
- スケジュール済みレポートの削除

SFR の 1 回のみの配信のスケジュール設定

SonicFlow レポート (SFR) の 1 回のみの配信をスケジュール設定するには、以下の手順に従います

1. 「**スケジュール種別**」で、「**1 回**」を選択します。

2. 「**1 回**」セクションで、SFR を作成する期間を設定します。ドロップダウン メニューから年、月、日、時、分を選択し、レポートの**開始**期間と**終了**期間を設定します。
3. 「**保存**」をクリックします。

SFR の繰り返し配信のスケジュール設定

SonicFlow レポート (SFR) の繰り返し配信をスケジュールするには、以下の手順に従います

1. 「**スケジュール種別**」で、「**繰り返し**」を選択します。
2. 「**繰り返し**」セクションで、以下の操作を行います。

   a. レポートを作成する曜日を選択します。すべての曜日を一度に選択するには「**すべて**」を選択します。
   b. レポートの**開始時刻**と**終了時刻**を 24 時間形式 (午前 2 時は 02:00、午後 2 時は 14:00 など) で入力します。
   c. 「**追加**」を選択して、レポートを「**スケジュール リスト**」に追加します。
   d. 作成するスケジュール済みレポートごとにこれらの手順を繰り返します。
3. 「OK」をクリックします。

スケジュール済みレポートの削除

一部またはすべてのスケジュール済みレポートを削除できます。

特定のスケジュール済みレポートを削除するには、以下の手順に従います

1. 削除するレポートを「**スケジュール リスト**」で選択します。
2. 「**このスケジュールの削除**」(小さいごみ箱) をクリックします。選択したレポートがリストから削除されます。

すべてのスケジュール済みレポートを削除するには、以下の手順に従います

1. 「**すべて削除**」(上部のごみ箱) をクリックします。すべてのレポートがリストから削除されます。

NetFlow の有効化と配備の情報

SonicWall は、計画、監視、およびアカウンティング アプリケーションに必要なデータをキャプチャする、戦略的に配置されたエッジ/アグリゲーション ルータ上での NetFlow の配備と NetFlow サービスの有効化について慎重に計画を立てることをお勧めします。配備に関する重要な考慮事項としては以下のものがあります。

- アプリケーション主導のデータ収集要件を理解する: アカウンティング アプリケーションにはルータ フローの開始と終了の情報だけで済むこともあるのに対し、アプリケーションの監視では、より包括的な (データ集約型の) エンド ツー エンド ビューが必要になることもあります。
- ネットワークトポロジおよびルーティング ポリシーがフロー収集戦略へあたえる影響を理解する: たとえば、重複したフローの収集を避けるため、トラフィックの開始点または終了点となる要のアグリゲーション ルータ上で NetFlow を有効化し、同じフロー情報の重複ビューを生じさせるバックボーン ルータや中間ルータでは有効化しません。
- NetFlow を SonicOS/X 管理インターフェースに実装して、ネットワーク内のフロー数およびルータへの影響を把握できます。その後、NetFlow エクスポートをセットアップして、NetFlow の展開を完了することができます。

一般に、NetFlow はエッジ/アグリゲーション ルータまたは WAN アクセス ルータの適切なインターフェースに配備すべき受信測定技術であり、アカウンティング、監視、およびネットワーク計画のデータに関する顧客のニーズを満たすためにトラフィックの開始と終了についての包括的なビューを得るためのものです。NetFlow によるデータ量の管理性を高めるための重要な手法は、NetFlow の配備を慎重に計画することです。NetFlow をネットワーク内のすべてのルータに配備する代わりに、段階的 (つまり、インターフェース単位で) かつ戦略的に (つまり、適切なルータに対して) 配備できます。

ユーザ設定タスク

収集するフローの種別に応じて、セットアップと構成に最適な報告の種別を決定する必要があります。このセクションでは、サポートされている各 NetFlow ソリューションの構成例と、2 台目の装置をコレクターとして動作させる構成を含みます。

- NetFlow バージョン 5 の設定
- NetFlow バージョン 9 の設定
- IPFIX (NetFlow バージョン 10) の設定
- 拡張 IPFIX の設定
- IPFIX を介してログを含めるための AppFlow エージェントの設定
- SonicWall Scrutinizer を用いる拡張 NetFlow の設定

NetFlow バージョン 5 の設定

Netflow バージョン 5 のフロー報告を構成するには、以下の手順に従います

1. 「**設定**」を選択します。
2. 「**設定**」セクションの「**接続報告**」で、次の 3 つのラジオ ボタンのいずれかを選択します。
   - **すべて**（既定）
   - **インターフェース基準** – 有効にすると、フロー報告は、始動または応答インターフェースを基準として行われます。
   - **ファイアウォール/アプリケーション ルール基準** – 有効にすると、既存のファイアウォール ルールを基準とするフロー報告が行われます。

   有効になっている場合、フロー報告は、始動または応答インターフェース、あるいは既存のファイアウォール ルールを基準として行われます。

   ⓘ **補足:** この手順は*オプション*ですが、選択したインターフェースでフロー報告が行われる場合は必須です。
3. 「**外部コレクター**」タブを選択します。
4. 「**フローとリアルタイム データを外部コレクターに送信する**」を選択します。
5. 「**外部フロー報告形式**」として、ドロップダウン リストから「**Netflow バージョン 5**」を選択します。
6. 「**外部コレクター サーバ アドレス**」フィールドで外部コレクターの IP アドレスを指定します。
7. 必要に応じて、VPN トンネルで外部コレクターに到達しなければならない場合は、「**VPN トンネルでコレクターを使用する際の送信元 IP**」に送信元 IP を指定します。

   ⓘ **重要:** VPN トンネルによって外部コレクターに到達する必要がある場合、この手順は*必須*です。
8. 「**外部コレクター UDP ポート番号**」で外部コレクターの UDP ポート番号を指定します。既定のポートは 2055 です。
9. 「**適用**」を選択します。

   ⓘ **補足:** この構成を有効にするために、装置の再起動が必要になることがあります。

NetFlow バージョン 9 の設定

Netflow バージョン 9 のフロー報告を構成するには、以下の手順に従います

1. 「**設定**」を選択します。
2. 「**設定**」セクションの「**接続報告**」で、次の 3 つのラジオ ボタンのいずれかを選択します。
   - **すべて**（既定）
   - **インターフェース基準** – 有効にすると、フロー報告は、始動または応答インターフェースを基準として行われます。
   - **ファイアウォール/アプリケーション ルール基準** – 有効にすると、既存のファイアウォール ルールを基準とするフロー報告が行われます。

   ⓘ **重要:** この手順はオプションですが、選択したインターフェースでフロー報告が行われる場合は必須です。
3. 「**外部コレクター**」を選択します。
4. 「**フローとリアルタイム データを外部コレクターに送信する**」を選択します。

ⓘ | **重要:** このオプションを有効にすると、この機能を有効にするために装置の再起動が必要になることがあります。

5. 「**外部フロー報告形式**」として、ドロップダウン メニューから「**Netflow バージョン 9**」を選択します。
6. 「**外部コレクター サーバ アドレス**」フィールドで外部コレクターの IP アドレスを指定します。
7. 必要に応じて、VPN トンネルで外部コレクターに到達しなければならない場合は、「**VPN トンネルでコレクターを使用する際の送信元 IP**」に送信元 IP を指定します。

   ⓘ | **重要:** VPN トンネルによって外部コレクターに到達する必要がある場合、この手順は必須です。
8. 「**外部コレクター UDP ポート番号**」で外部コレクターの UDP ポート番号を指定します。既定のポートは 2055 です。
9. 「**動作**」で、「**すべてのテンプレートの生成**」をクリックしてテンプレートの生成を開始します。確認を求めるメッセージが表示されます。

   ⓘ | **重要:** IPFIX は、データを送信する前に外部コレクターに知らせる必要があるテンプレートを使います。
10. テンプレートが生成された後、「**適用**」を選択します。

IPFIX (NetFlow バージョン 10) の設定

IPFIX (Netflow バージョン 10) のフロー報告を構成するには、以下の手順に従います

1. 「**設定**」を選択します。
2. 「**設定**」セクションの「**接続報告**」で、次の 3 つのラジオ ボタンのいずれかを選択します。

   - **すべて**（既定）
   - **インターフェース基準** – 有効にすると、フロー報告は、始動または応答インターフェースを基準として行われます。
   - **ファイアウォール/アプリケーション ルール基準** – 有効にすると、既存のファイアウォール ルールを基準とするフロー報告が行われます。

   ⓘ | **重要:** この手順は*オプション*ですが、選択したインターフェースでフロー報告が行われる場合は*必須*です。
3. 「**外部コレクター**」を選択します。
4. 「**フローとリアルタイム データを外部コレクターに送信する**」を選択します。

   ⓘ | **重要:** このオプションを有効にすると、この機能を有効にするために装置の再起動が必要になることがあります。
5. 「**外部フロー報告形式**」として、ドロップダウン メニューから「**IPFIX**」を選択します。
6. 「**外部コレクターサーバアドレス**」フィールドで外部コレクターの IP アドレスを指定します。
7. 必要に応じて、VPN トンネルで外部コレクターに到達しなければならない場合は、「**VPN トンネルでコレクターを使用する際の送信元 IP**」に送信元 IP を指定します。

   ⓘ | **重要:** VPN トンネルによって外部コレクターに到達する必要がある場合、この手順は*必須*です。
8. 「**外部コレクター UDP ポート番号**」で外部コレクターの UDP ポート番号を指定します。既定のポートは **2055** です。
9. 「**動作**」で、「**すべてのテンプレートの生成**」をクリックしてテンプレートの生成を開始します。確認を求めるメッセージが表示されます。

   ⓘ | **重要:** IPFIX は、データを送信する前に外部コレクターに知らせる必要があるテンプレートを使います。
10. テンプレートが生成された後、「**適用**」を選択します。

拡張 IPFIX の設定

拡張 IPFIX のフロー報告を構成するには、以下の手順に従います、以下の手順に従います

1. 「**設定**」を選択します。
2. 「**設定**」セクションの「**接続報告**」で、次の 3 つのラジオ ボタンのいずれかを選択します。
   - **すべて**（既定）
   - **インターフェース基準** – 有効にすると、フロー報告は、始動または応答インターフェースを基準として行われます。
   - **ファイアウォール/アプリケーション ルール基準** – 有効にすると、既存のファイアウォール ルールを基準とするフロー報告が行われます。

   ⓘ **重要:** この手順は*オプション*ですが、選択したインターフェースでフロー報告が行われる場合は*必須*です。
3. 「**外部コレクター**」を選択します。
4. 「**フローとリアルタイム データを外部コレクターに送信する**」を選択します。

   ⓘ **重要:** このオプションを有効にすると、この機能を有効にするために装置の再起動が必要になることがあります。
5. 「**外部フロー報告形式**」ドロップダウン メニューから「**拡張 IPFIX**」を選択します。
6. 「**外部コレクターサーバアドレス**」フィールドで外部コレクターの IP アドレスを指定します。
7. VPN トンネルで外部コレクターに到達しなければならない場合は、「**VPN トンネルでコレクターを使用する際の送信元 IP**」に送信元 IP を指定します。

   ⓘ **重要:** VPN トンネルによって外部コレクターに到達する必要がある場合、この手順は*必須*です。
8. 「**外部コレクター UDP ポート番号**」で外部コレクターの UDP ポート番号を指定します。既定のポートは **2055** です。
9. 「**以下のテーブルに静的 AppFlow を送信する**」ドロップダウン メニューから、静的フローを受信したいテーブルを選択します。
10. 「**以下のテーブルに動的 AppFlow を送信する**」ドロップダウン メニューから、動的フローを受信したいテーブルを選択します。
11. 「**IPFIX に以下の追加報告を含む**」ドロップダウン メニューから、フローに対して生成する追加の報告を選択します。

    ⓘ **重要:** システム ログを生成するには、このドロップダウン メニューから「システム ログ」を選択します。
12. 「すべてのテンプレートの生成」をクリックしてテンプレートの生成を開始します。

    ⓘ **重要:** 拡張 IPFIX は、データを送信する前に外部コレクターに通知する必要があるテンプレートを使います。
13. 「**定期的に静的 AppFlow を送信する**」チェックボックスを選択して、このオプションを有効にします。このオプションを有効にした後で、「**静的フローを生成する**」をクリックします。
14. 静的フロー データの生成を開始するには、「**静的 AppFlow データを生成する**」をクリックします。確認を求めるメッセージが表示されます。
15. ログ メッセージを外部コレクターに送信するには、「**外部コレクターにログ設定を送信する**」オプションの「**登録をすべて送信**」をクリックします。

    ⓘ **重要:** 「**登録をすべて送信**」ボタンを選択する前に、ファイアウォールの SonicOS/X と外部コレクター サーバの接続が完了していることを確認してください。

外部サーバは、再起動時に使用するプロパティ(「保存されるプロパティ」を参照)と設定を読み込みます。以下の場合は、「**登録をすべて送信**」をクリックして設定を同期します。

- SonicOS/X のアップグレードなどによってログ イベントが新たに追加された場合。
- SonicOS/X (ファイアウォール)と外部サーバの接続がしばらく停止し、その間にログ設定が編集された可能性がある場合。

ⓘ **補足:** ログ イベント設定のフィールドが変更された場合、SonicOS/X は自動的に更新を外部サーバに送信します。

保存されるプロパティ

種別	プロパティ	
イベントのプロパティと設定	イベント ID 所属グループ ID 色 メッセージ種別 ID	優先順位 ストリーム フィルタ イベント名 ログ メッセージ
グループのプロパティ	グループ ID 所属種別 ID	グループ名
種別のプロパティ	種別 ID	種別名
メッセージ種別のプロパティ	種別 ID	種別名

16. 「**適用**」を選択します。

IPFIX を介してログを含めるための AppFlow エージェントの設定

IPFIX を介してログを含めるために AppFlow エージェントを構成するには、以下の手順に従います

1. 「**デバイス | Appflow > フロー報告**」に移動します。
2. 「**AppFlow エージェント**」をクリックします。
3. 「**SonicWall AppFlow エージェントにシステム ログを送信する**」を選択します。このオプションは、既定では選択されていません。
4. 「**適用**」を選択します。
5. 「**デバイス | Appflow > AppFlow エージェント**」に移動します。
6. ログ メッセージを AppFlow エージェントに送信するには、「**ログ設定の同期**」をクリックします。

   ⓘ **重要:** 「**ログ設定の同期**」をクリックする前に、ファイアウォールの SonicOS/X と AppFlow エージェント サーバとの接続準備が完了していることを確認してください。

   外部サーバは、再起動時に使用するプロパティ(「保存されるプロパティ」を参照)と設定を読み込みます。以下の場合は、「**すべての登録を送信**」をクリックして設定を同期します。

   - SonicOS/X のアップグレードなどによってログ イベントが新たに追加された場合。
   - SonicOS/X (ファイアウォール)と外部サーバの接続がしばらく停止し、その間にログ設定が編集された可能性がある場合。

   ⓘ **補足:** ログ イベント設定のフィールドが変更された場合、SonicOS/X は自動的に更新を外部サーバに送信します。
7. 「**適用**」を選択します。

SonicWall Scrutinizer を用いる拡張 NetFlow の設定

拡張 Netflow で使用できる外部フロー報告オプションの 1 つとして、SonicWall Scrutinizer というサードパーティ製コレクターがあります。このコレクターは、Netflow および SonicWall フローの両方に対応した一定の範囲の報告と分析を表示します。

拡張 Netflow の報告の設定を確認するには、以下の手順に従います

1. 「**設定**」を選択します。
2. 「**設定**」セクションの「**接続報告**」で、「**すべて**」を選択します。

   ⓘ **重要:** この手順はオプションですが、選択したインターフェースでフロー報告が行われる場合は必須です。
3. 「**外部コレクター**」を選択します。
4. 「**フローとリアルタイム データを外部コレクターに送信する**」をクリックします。

   ⓘ **重要:** このオプションを有効にすると、この機能を有効にするために装置の再起動が必要になることがあります。
5. 「**外部フロー報告形式**」ドロップダウン メニューから「拡張 IPFIX」を選択します。
6. 「**外部コレクターサーバアドレス**」フィールドで外部コレクターの IP アドレスを指定します。
7. 必要に応じて、VPN トンネルによって外部コレクターに到達する必要がある場合は、「**VPN トンネルでコレクターを使用する際の送信元 IP**」フィールドで送信元 IP を指定します。

   ⓘ **重要:** VPN トンネルによって外部コレクターに到達する必要がある場合、この手順は*必須*です。
8. 「**外部コレクター UDP ポート番号**」で外部コレクターの UDP ポート番号を指定します。既定のポートは **2055** です。
9. 「**定期的に静的 AppFlow を送信する**」をクリックします。
10. 「**以下のテーブルに動的 AppFlow を送信する**」ドロップダウン メニューから、静的フローを受信したいテーブルを選択します。

    ⓘ **補足:** 現在、Scrutinizer は「アプリケーション」と「脅威」のみをサポートしています。Plixer は、将来のバージョンで静的フローの「ロケーション マップ」、「サービス」、「格付けマップ」、「テーブル マップ」、および「カラム マップ」をサポートする予定です。
11. 「**静的 AppFlow データを生成する**」をクリックします。
12. 「**適用**」を選択します。
13. 「**ネットワーク | システム > インターフェース**」に移動します。
14. データの要求先となるすべてのインターフェースについて、**構成**アイコンをクリックして「**フロー報告**」が有効になっていることを確認します。「**インターフェースの編集**」ダイアログが表示されます。
15. 「**詳細**」タブで、「**フロー報告を有効にする**」が選択されていることを確認します。
16. 「**OK**」をクリックします。
17. SonicWall Scrutinizer にログインします。数分でデータが表示されます。

NetFlow テーブル

次のセクションでは、種々の NetFlow テーブルについて説明します。また、フローを報告するようにSonicWall を構成した場合にエクスポートされる拡張 IPFX テーブルについても詳しく説明します。

トピック:

静的テーブル

静的テーブルとは、時間が経過してもデータが変化しないテーブルです。ただし、このデータは他のテーブルと関連付けるために不可欠です。静的テーブルは、通常は指定の間隔で報告されますが、1 度だけ送信されるように構成することもできます。「エクスポートできる静的 IPFIX テーブル」は、エクスポートできる静的 IPFIX テーブルの一覧を示します。

エクスポートできる静的 IPFIX テーブル

アプリケーション マップ	種々の属性、シグネチャ ID、アプリケーション ID、種別名、および種別 ID など、ファイアウォールが識別するすべてのアプリケーションを報告します。
ウイルス マップ	ファイアウォールによって検知されたすべてのウイルスを報告します。
スパイウェア マップ	ファイアウォールによって検知されたすべてのスパイウェアを報告します。
侵入マップ	ファイアウォールによって検知されたすべての侵入を報告します。
ロケーション マップ	国と地域およびそれらの ID のリストを記述した SonicWall のロケーション マップを表します。
サービス マップ	ポート番号、プロトコル種別、ポート番号の範囲、および名前が含まれる SonicWall のサービス リストを表します。
格付けマップ	SonicWall の格付け ID リストおよび格付け種別の名前を表します。
テーブル レイアウト マップ	テーブル ID とテーブル名など、エクスポートする SonicWall のテーブルのリストを報告します。
カラム マップ	すべてのテーブルの各カラムについて名前、種別サイズ、および IPFIX 標準相当と共に報告する SonicWall のカラム リストを表します。

動的テーブル

動的テーブルのデータは、静的テーブルとは違って、時間が経過すると変化し、ファイアウォールの動作に基づいて繰り返し送信されます。これらのテーブルのカラムは、統計や使用率の報告が含まれる少数のテーブルを除い

て、時間の経過と共に増大します。「エクスポートできる動的 IPFIX テーブル」は、エクスポートできる動的 IPFIX テーブルの一覧を示します。

エクスポートできる動的 IPFIX テーブル

接続	SonicWall の接続を報告します。トリガを設定することによって、同じフロー テーブルを何回も報告することができます。
ユーザ	LDAP/RADIUS、ローカル、または SSO を介してファイアウォールにログインしているユーザを報告します。
URL	ファイアウォールを通じてアクセスされた URL を報告します。
URL 格付け	ファイアウォールを通じてアクセスされたすべての URL の格付け ID を報告します。
VPN	ファイアウォールを通じて確立されたすべての VPN トンネルを報告します。
デバイス	接続されたデバイスの MAC アドレス、IP アドレス、インターフェース、および NETBIOS 名を含めて、ファイアウォールを通じて接続されたすべてのデバイスのリストを報告します。
スパム	スパム サービスを通したすべての電子メール交換を報告します。
位置	IP アドレスのロケーションとドメイン名を報告します。
VoIP	ファイアウォールを通じたすべての VoIP/H323 呼び出しを報告します。

テンプレート

これは、エクスポートされる Netflow テンプレート テーブル種別の例を示します。独自の Netflow 構成の診断レポートを実行するには、「**デバイス | 診断 > テクニカル サポート レポート**」に移動し、「**動作**」セクションの「**テクニカル サポート レポートのダウンロード**」をクリックします。

トピック:

- NetFlow バージョン 5
- NetFlow バージョン 9
- IPFIX (NetFlow バージョン 10)
- 拡張 IPFIX

NetFlow バージョン 5

NetFlow バージョン 5 のデータグラムは、ヘッダーと 1 つ以上のフロー レコードから成っており、UDP を使用してエクスポート データグラムを送信します。ヘッダーの最初のフィールドには、エクスポート データグラムのバージョン番号が含まれます。ヘッダーの 2 番目のフィールドには、データグラム内のレコード数が含まれます。これはレコードの検索に使用できます。NetFlow バージョン 5 は固定データグラムなので、テンプレートは使用できず、「NetFlow バージョン 5 のヘッダー形式」および「NetFlow バージョン 5 のヘッダー形式」の表に記載される形式に従います。

NETFLOW バージョン 5 のヘッダー形式

バイト	内容	説明
0–1	version	NetFlow エクスポート形式のバージョン番号
2–3	count	このパケットでエクスポートされたフローの数 (1～30)
4–7	SysUptime	エクスポート デバイスが起動してから現在までの時間 (ミリ秒数)
8–11	unix_secs	0000 UTC 1970 から現在までの秒数
12–15	unix_nsecs	0000 UTC 1970 からの残余時間 (ナノ秒数)
16–19	flow_sequence	観測したフロー全体のシーケンス カウンタ
20	engine_type	フロー スイッチング エンジンの種別
20	engine_id	フロー スイッチング エンジンのスロット番号
22–23	sampling_interval	最初の 2 ビットがサンプリング モードを保持し、残りの 14 ビットがサンプリング間隔の値を保持します。

NETFLOW バージョン 5 のレコード形式

バイト	内容	説明
0–3	srcaddr	送信元 IP アドレス
4–7	dstaddr	送信先 IP アドレス
8–11	nexthop	ネクスト ホップ ルータの IP アドレス
12–13	input	入力インターフェースの SNMP インデックス
14–15	output	出力インターフェースの SNMP インデックス
10–19	dPkts	フローのパケット数
20–23	dOctets	フローのパケットのレイヤ 3 バイトの総数
24–27	First	フロー開始時の SysUptime
28–31	Last	フローの最終パケット受信時の SysUptime
32–33	srcport	TCP/UDP 送信元ポート番号または同等の情報
34–35	dstport	TCP/UDP 送信先ポート番号または同等の情報

バイト	内容	説明
36	pad1	未使用（ゼロ）バイト
37	tcp_flags	TCP フラグの累積 OR
38	prot	IP プロトコル種別（例えば、TCP=6、UDP=17）
39	tos	IP サービス種別（ToS）
40–41	src_as	送信元のAutonomous システム番号（起点またはピアのいずれか）
42–43	dst_as	送信先のAutonomousシステム番号（起点またはピアのいずれか）
44	src_mask	送信元アドレス プレフィックス マスク ビット
45	dst_mask	送信先アドレス プレフィックス マスク ビット
46–47	pad2	未使用（ゼロ）バイト

NetFlow バージョン 9

NETFLOW バージョン 9 の例

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

「NetFlow バージョン 9 のテンプレート FlowSet フィールド」は、NetFlow バージョン 9 のテンプレート FlowSet フィールドの詳細です。

NETFLOW バージョン 9 のテンプレート FLOWSET フィールド

フィールド名	説明
テンプレート ID	ファイアウォールは、エクスポートされる NetFlow データのタイプに適合する FlowSet テンプレートに基づいて一意の ID を持つテンプレートを生成します。
名前	NetFlow テンプレートの名前。
エレメント数	NetFlow テンプレート内のフィールドの総数。
総バイト長	NetFlow テンプレート内の報告されたすべてのフィールドの総バイト長。
フィールド種別	フィールドの種別を表す数値。この値はベンダーごとに異なる可能性があります。
フィールドバイト長	特定のフィールド種別のバイト長。

IPFIX (NetFlow バージョン 10)

IPFIX (NETFLOW バージョン 10) の例

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

「IPFIX のテンプレート FlowSet フィールド」は、IPFIX のテンプレート FlowSet フィールドの詳細です。

IPFIX のテンプレート FLOWSET フィールド

フィールド名	説明
テンプレート ID	ファイアウォールは、エクスポートされる NetFlow データのタイプに適合する FlowSet テンプレートに基づいて一意の ID を持つテンプレートを生成します。
名前	NetFlow テンプレートの名前。
エレメント数	NetFlow テンプレート内のフィールドの総数。
総バイト長	NetFlow テンプレート内の報告されたすべてのフィールドの総バイト長。
フィールド種別	フィールド種別はフィールドの種別を表す数値です。この値はベンダーごとに異なる可能性があります。
種別バイト長	特定のフィールド種別のバイト長。

拡張 IPFIX

拡張 IPFIX がエクスポートするテンプレートは、前述したバージョンの NetFlow フィールドと SonicWall ID を組み合わせたものです。これらのフローには、エンタープライズ定義のフィールド タイプやエンタープライズ ID といった拡張がいくつか含まれています。

ⓘ | **補足:** SonicWall 固有のエンタープライズ ID (EntID) は 8741 として定義されています。

「拡張 IPFIX 名のテンプレートの例」は拡張 IPFIX テンプレートの標準です。指定されている値は静的で、すべてのエクスポート可能な NetFlow テンプレートのテーブル名と関連しています。「拡張 IPFIX のテンプレートの例」も参照してください。

拡張 IPFIX 名のテンプレートの例

```
STATIC TABLES
-----------------

Table MAP table
 Table(Template) Id=256, Table Name=Flow IPFIX
 Table(Template) Id=257, Table Name=Flow IPFIX extn
 Table(Template) Id=258, Table Name=Table Map
 Table(Template) Id=259, Table Name=Column Map
 Table(Template) Id=260, Table Name=User
 Table(Template) Id=261, Table Name=Application
 Table(Template) Id=262, Table Name=URL
 Table(Template) Id=263, Table Name=Rating
 Table(Template) Id=264, Table Name=IPS
 Table(Template) Id=265, Table Name=GAV
 Table(Template) Id=266, Table Name=Anti Spyware
 Table(Template) Id=267, Table Name=Location Map
 Table(Template) Id=268, Table Name=Location
 Table(Template) Id=269, Table Name=Log
 Table(Template) Id=270, Table Name=if-stat
 Table(Template) Id=271, Table Name=core-stat
 Table(Template) Id=272, Table Name=Voip
 Table(Template) Id=273, Table Name=Services
 Table(Template) Id=274, Table Name=Spam
 Table(Template) Id=275, Table Name=memory
 Table(Template) Id=276, Table Name=devices
 Table(Template) Id=277, Table Name=vpn tunnels
 Table(Template) Id=278, Table Name=URL rating
```

拡張 IPFIX のテンプレートの例

```
IPFix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
 EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
 EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
 EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
 EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
 EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
 EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
 EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator GW-IP Addr
 EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder GW-IP Addr
 EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
 EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
 EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
 EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
 EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
 EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
 EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
 EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
 EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
 EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
 EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
 EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
 EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
 EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
 EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
 EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
 EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
 EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
 EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
 EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
 EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
 EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
 EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
 EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
 EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
 EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
 EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
 EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
 EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
 EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
 EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
 EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
 EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
 EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
 EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID
```

2

AppFlow エージェント

この画面では、AppFlow およびリアルタイム データを AppFlow エージェントに送信できます。AppFlow エージェントは、SonicWall Flow Analytics、GMS または NSM のいずれかです。

AppFlow およびリアルタイム データを AppFlow エージェントに送信するには、以下の手順に従います

1. 「**デバイス | Appflow > AppFlow エージェント**」に移動します。

2. 「**Flow サーバ設定モード**」で、「**基本**」または「**詳細**」モードを選択します。「**詳細**」を選択すると、「**詳細設定**」オプションが使用可能になり、代替 Flow サーバと詳細フロー設定を構成することができます。
3. 「**AppFlow エージェントを自動同期する**」の場合、AppFlow エージェントは「AppFlow 監視」、「AppFlow 報告」、「AppFlow ダッシュボード」に表示する前に静的データをファイアウォールからそのデータを取得する必要があります。このチェックボックスを有効にすると、ファイアウォールは自動的に AppFlow エージェントとデータを同期します。
4. 「**詳細 Flow サーバ設定モード**」の場合、「**アクティブ スタンバイ**」モードを使用すると、フローは AppFlow エージェント 1（AppFlow エージェント 1 が稼働中の場合）へ誘導されます。AppFlow エージェント 1 が休止中で、AppFlow エージェント 2 が稼働中の場合、フローは AppFlow エージェント 2 へ誘導されます。「**負荷分散**」モードでは、「**負荷分散モード**」、「**ミラー**」、「**共有負荷**」の中から選択できます。これらのラジオ ボタンは、「**負荷分散**」モードが選択されている場合に限り有効になります。「**共有負荷**」が選択されており、どちらの Flow サーバも**稼働中**の場合、フローはこの 2 台の AppFlow エージェントに均等に分割されます。ミラーを選択すると、すべてのフローは両方の Flow サーバに送信されます。

5. 「**AppFlow エージェント 1**」および「**AppFlow エージェント 2**」内で、「**AppFlow エージェント アドレス**」オプションの「**IP**」を選択すると、デバイスは AppFlow よびリアルタイム データを指定された IP アドレス/アドレス オブジェクトに送信します。AppFlow エージェントが VPN トンネル経由で到達可能な場合、VPN トンネルに使用する送信元 IP を指定できます。使用できるアドレス オブジェクトの種別は、**ホスト**または **FQDN** のみです。
6. 「**VPN トンネルを超えて使用する送信元 IP**」オプションでは、AppFlow エージェントが VPN トンネル経由で到達可能な場合、その IP アドレスをここで指定できます。VPN ポリシーから IP を選択します。
7. 「**サーバ通信タイムアウト**」を使用すると、データはダッシュボードにリダイレクトされます。SonicWall ファイアウォールの GUI を使用して、ダッシュボード データを AppFlow エージェントから取得できます。指定されたタイムアウトは、AppFlow エージェントからデータを取得する際、エラーになるまで待機する秒数です。最小値は 60、最大値は 120、既定値は 60 です。
8. 「**接続テスト**」を選択すると、AppFlow エージェントに接続して登録情報、イメージ バージョン、カウンターを収集します。
9. 「**サーバの同期**」オプションを使用すると、静的データを手動で AppFlow エージェントに送信できます。これは、AppFlow エージェントを起動してファイアウォールを登録した後に 1 回のみ実行できます。
10. 「**ログ設定の同期**」を選択すると、必要なログ設定のフィールドを AppFlow エージェントに送信し、ログを表示します。

AppFlow エージェントへの接続

「**デバイス | AppFlow > AppFlow エージェント**」ページでは、AppFlow エージェントへの接続を確立できます。

AppFlow エージェントの役割は、分散環境における展開で使用できます。この役割では、AppFlow エージェントが単一のサービスとして実行され、既定のポートで SonicWall フローを収集します。

この役割で動作する単一のサービスは、SonicWall Universal Management Suite – フロー サーバです。フローは、内部データベースに収集され、保存されます。これらのフローからレポートを作成するには、AppFlow エージェントを配備し、「**コンソール**」または「**オール イン ワン**」の役割を設定する必要があります。また、以下のポートをオープンにする必要もあります。

- UDP 2055
- UDP 5055
- TCP 9063
- TCP 9064
- TCP 9065
- TCP 9066
- TCP 9067

AppFlow エージェントには、固定の Syslog ファシリティ（ローカル 0）、Syslog 形式（既定）、および サーバ ID（ファイアウォール）があります。AppFlow エージェントのイベント プロファイル値は既定で 0 に設定されますが、プロファイルに関係なくすべてのイベントが AppFlow エージェントに報告されます。AppFlow エージェントは、速度制限からも除外されます。AppFlow エージェントを有効/無効にできるのは、「**デバイス | AppFlow > フロー報告 | 設定**」ページの「より高度な管理」セクションのみです。「**デバイス | ログ > Syslog**」ページでは有効/無効を切り換えることはできません。

トピック:

基本モード

接続の確立は、次の 2 ステップで行われます。

1. AppFlow エージェントへの接続を確立します。
2. SonicOS/X の「**ログとレポート | AppFlow 設定 > フロー報告**」ページで AppFlow エージェントを構成します。

GMS を使用した AppFlow エージェントの設定に関する詳細は、最新の SonicWall GMS または『SonicWall 管理サービス管理マニュアル』（https://www.sonicwall.com/ja-jp/support/technical-documentation でダウンロード可能）を参照してください。

AppFlow エージェントへの接続を確立するには、以下の手順に従います

1. インスタント AppFlow エージェントにログインします。
2. 「**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。
3. AppFlow エージェントのホスト IP アドレスを見つけてコピーします。

SonicWall ネットワーク セキュリティ装置で、以下の手順に従います。

1. 「**デバイス | Appflow > AppFlow エージェント**」ページに移動します。
2. 「**Flow サーバ設定モード**」で、「**基本**」が選択されている必要があります（これが既定の設定です）。

3. 「**AppFlow エージェント アドレス**」フィールドで、以下のいずれかを実行します。
   - AppFlow エージェントからコピーしたホスト IP アドレスを貼り付けます。
   - 事前定義されたアドレス オブジェクトを「**AddrObj**」ドロップダウン メニューから選択します。「**アドレス オブジェクトの作成**」を選択して新しいアドレス オブジェクトを作成することもできます。
4. 「**VPN トンネルを越えて使用する送信元 IP**」フィールドに、適用可能な VPN ポリシーの送信元 IP アドレスを指定します。

   ⓘ **重要:** AppFlow エージェントが VPN トンネル経由で到達可能な場合、このフィールドを指定する必要があります。VPN ポリシーから IP を選択できます。
5. 「**サーバ通信タイムアウト**」フィールドに、Flow サーバからの応答をファイアウォールが待機する時間（秒数）を指定します。有効な範囲は **60**（既定値）～ **120** 秒です。
6. ファイアウォールが再起動するたびに静的なフローをフロー サーバに送信する場合は、「**GMSFlow サーバを自動同期する**」オプションを選択します。（これは既定で選択されています）。
7. AppFlow エージェントへの接続をテストするには、「**接続テスト**」をクリックします。接続状況が表示されます。
8. 静的データを AppFlow エージェントに手動で送信する場合は、「**サーバの同期**」をクリックします。同期状況が表示されます。

   ⓘ **重要:** SonicWall AppFlow エージェントに接続して登録した後で、「**サーバの同期**」を 1 回だけクリックする必要があります。
9. 「**適用**」を選択します。

トピック:

- AppFlow エージェントへの接続
- 詳細モード

詳細モード

詳細設定モードでは、複数の AppFlow エージェントを選択し、サーバ間でフローをどのように振り向けたり負荷分散したりするかを設定できます。

接続の確立は、次の 2 ステップで行われます。

1. AppFlow エージェントへの接続を確立します。
2. 「**デバイス | AppFlow > フロー報告**」ページで AppFlow エージェントを構成します。

   GMS を使用した AppFlow サーバの設定に関する詳細は、最新の SonicWall GMS または『SonicWall 管理サービス管理マニュアル』(https://www.sonicwall.com/ja-jp/support/technical-documentation でダウンロード可能)を参照してください。

AppFlow エージェントへの接続を確立するには、以下の手順に従います

1. GMS で、インスタント AppFlow エージェントにログインします。
2. 「**ネットワーク > 設定**」ページに移動します。
3. AppFlow エージェントのホスト IP アドレスを見つけてコピーします。

SonicWall ネットワーク セキュリティ装置で、以下の手順に従います。

1. 「**デバイス | Appflow > AppFlow エージェント**」ページに移動します。
2. 「**AppFlow エージェント構成モード**」で、「**詳細**」を選択します。
3. 「**詳細フロー サーバ構成モード**」を設定します。
   - **アクティブスタンバイ** – このオプションを選択すると、フローは最初に AppFlow エージェント 1 へ誘導されます(利用可能な場合)。AppFlow エージェント 1 が利用できない場合、フローは AppFlow エージェント 2 へ誘導されます(利用可能な場合)。(これが既定の設定です)。
   - **負荷分散** – このオプションを選択すると、次のどちらかの負荷分散設定を選択できます。
     - **共有負荷** – 両方の Flow サーバが利用できる場合、フローは 2 台の Flow サーバ間で均等に分割されます。
     - **ミラー** – この負荷分散オプションを選択すると、すべてのフローが両方の Flow サーバに送られます。
4. 「**AppFlow エージェント アドレス**」フィールドで、以下のいずれかを実行します。
   - AppFlow エージェントからコピーしたホスト IP アドレスを貼り付けます。
   - 事前定義されたアドレス オブジェクトを「**AddrObj**」ドロップダウン メニューから選択します。「**アドレス オブジェクトの作成**」を選択して新しいアドレス オブジェクトを作成することもできます。
5. 各 AppFlow エージェントの「**VPN トンネルを越えて使用する送信元 IP**」フィールドに、適用可能な VPN ポリシーの送信元 IP アドレスを指定します。

   ⓘ **重要:** AppFlow エージェントが VPN トンネル経由で到達可能な場合、このフィールドを指定する必要があります。VPN ポリシーから IP を選択できます。
6. 各 AppFlow エージェントの「**サーバ通信タイムアウト**」フィールドに、Flow サーバからの応答をファイアウォールが待機する時間(秒数)を指定します。有効な範囲は 60(既定値)～ 120 秒です。
7. ファイアウォールが再起動するたびに静的なフローを Flow サーバに送信できるようにする場合は、その AppFlow エージェントの「**Flow サーバを自動同期する**」オプションを選択します。
8. AppFlow エージェントへの接続をテストするには、その AppFlow エージェントの「**接続テスト**」をクリックします。接続状況が表示されます。
9. 静的データを AppFlow エージェントに手動で送信する場合は、その AppFlow エージェントの「**サーバの同期**」をクリックします。同期状況が表示されます。

   ⓘ **重要:** SonicWall GMS 製品に接続して登録した後で、「**サーバの同期**」を一度だけクリックする必要があります。
10. 「**適用**」を選択します。

トピック:

- AppFlow エージェントへの接続
- 基本モード

3

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 および SonicOSX デバイス AppFlow 管理者ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005636-00 Rev B

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