



トラフィック処理の概要

はじめに

ここでは、Service Control Engine (SCE) プラットフォームにインストールした Cisco Service Control Application for Broadband (SCA BB) でトラフィックを処理する方法を説明します。

また、SCA BB システムの主な要素（サービス コンフィギュレーション エンティティ）と相互の関連性についても説明します。

- 「ルーティング環境」 (P.3-1)
- 「トラフィック処理」 (P.3-2)
- 「トラフィックの分類」 (P.3-2)
- 「トラフィックのアカウントティングとレポート」 (P.3-9)
- 「トラフィックの制御」 (P.3-13)
- 「その他のトラフィック処理機能」 (P.3-18)
- 「サービス コンフィギュレーション」 (P.3-21)

ルーティング環境

トラフィック処理はルーティング環境によって異なります。シスコの Service Control ソリューションは次に示す 2 つの標準的なルーティング方法で動作可能です。

- 対称（通常）：インバウンドとアウトバウンドのほとんどのトラフィック フローが 1 つの SCE プラットフォームを通じてルーティングされます。この SCE プラットフォームを単方向だけしか通過しないフローはごくわずかです。
- 非対称：多くのフローは、この SCE プラットフォームを通じて一方向のトラフィック（インバウンドまたはアウトバウンド）だけがルーティングされます。他のフローは、両方向のトラフィックがこの SCE プラットフォームを通過します。

あるフローのインバウンドとアウトバウンドのトラフィックが同じ SCE プラットフォームを通過する場合、そのフローを双方向であるといいます。その SCE プラットフォームをインバウンドトラフィックとアウトバウンドトラフィックのいずれか一方だけ通過する場合は単方向フローです。

Cisco Service Control ソリューションは、単方向フローと双方向フローの両方を処理できます。SCE プラットフォームは、対称と非対称のいずれかのルーティング環境で動作するように設定できます。非対称環境の SCE プラットフォームのトラフィック処理能力は対称環境の能力の一部分です。

非対称ルーティング環境に Cisco Service Control ソリューションを配置して、単方向分類を有効にすると、SCE プラットフォームの分類機能は、単方向のトラフィックの識別精度がよくなります。SCE プラットフォームは単方向フローを独立して処理し、反対方向のフローを処理する可能性のある他の SCE プラットフォームと同期をとりません。

トラフィック処理

トラフィック処理には3つの段階があります。

- **トラフィックの分類**：SCA BB はトラフィック フローを分析し、それぞれのタイプを判別します（たとえば、ブラウジング、Eメール、ファイル共有、音声など）。
- **トラフィック アカウンティングとレポート**：SCA BB は課金処理を行い、Raw Data Record (RDR; 未加工データ レコード) を生成してネットワークを分析し、モニタします。
- **トラフィック制御**：SCA BB は、サービス、サブスクリバパッケージ、サブスクリバクォータの状態などに応じてトラフィック フローを制限し、優先順位を指定します。

詳細は以降のセクションで説明します。

分類、レポート、制御を変更するには、サービス コンフィギュレーションを編集して SCE プラットフォームに適用します。

トラフィックの分類

トラフィック処理はトラフィックの分類から始まり、これによってネットワーク セッションがサービス別に分類されます。

Service Control ソリューションには、プロバイダーがサブスクリバに提供する商用サービスに対応するサービスが定義されています。このサービスを使用して、トラフィックの分類と識別、トラフィックの使用状況に基づくレポート、トラフィックの制御が行えます。

- 「サービス」 (P.3-2)
- 「プロトコル」 (P.3-4)
- 「開始側」 (P.3-6)
- 「ゾーン」 (P.3-7)
- 「フレーバ」 (P.3-7)
- 「サービスへのフロー属性のマッピング」 (P.3-9)

サービス

トラフィックの分類では、SCA BB はネットワーク セッションをサービスに分類します。

サービスは次の2つの部分で構成されています。

- サービス コンフィギュレーション (SCA BB はサービスごとに異なる規則を適用できるため)
- 使用状況を集約したレポート

プロバイダーにとっては、サービスとはサブスクリバに販売するネットワーク製品です。通常はサブスクリバが使用するネットワークアプリケーションであり、ブラウジング、Eメール、ファイル共有、音声などがあります。技術的な観点からは、サービスは1つまたは複数のサービス要素で構成されています。それぞれのサービス要素によってサービスが決定され、ネットワークトラフィックフロータイプに関連付けられます。

デフォルトのサービスコンフィギュレーションには多数のサービスが定義されています（詳細については『Cisco Service Control Application for Broadband Reference Guide』の「Default Service Configuration Reference Tables」の章を参照してください）。サービスコンフィギュレーションのサービスは、変更することも追加することもできます。

サービスコンフィギュレーションには最大500件のサービスを設定できます。

セッションの開始と同時に分類が行われます。分類の際はセッションの最初の数パケットが検証され、セッションが所属するサービスが決定されます。次に、セッションにサービスIDが割り当てられます。サービスIDは、そのセッションが終了するまで変わりません。

トラフィックは次のサービス要素に基づいて分類され、サービスにマッピングされます。

- **プロトコル**：使用されるプロトコル。たとえば、ブラウジングフローとEメールフローをそれぞれのサービスにマッピングできます。
- **開始側**：フローを生成したサブスクリバ側またはネットワーク側。たとえば、サブスクリバ側とネットワーク側で開始されたピアツーピアトラフィックを、それぞれのサービスにマッピングできます。
- **ゾーン**：フローのネットワーク側ホストIPアドレスのリスト。たとえば、特定のサーバに送信されるすべての音声フローを特定のサービスにマッピングできます。
- **フレバ**：レイヤ7の特定のプロパティ。フローのネットワーク側ホストのホスト名などです。たとえば、一定のパターンと一致するURLのHTTPフローをすべて特定のサービスにマッピングできます。



(注) 単方向分類が有効になっている場合、フレバは分類には使用されません。

SCA BBは、このようなフローマッピングを使用して、SCA BBが通過するネットワーク接続をサービスにマッピングします。サービスごとに規則を定義し、制御ポリシーを実装できます。分類規則にはレイヤ3およびレイヤ4のパラメータ（ポート番号やIPアドレスなど）と、レイヤ7のパラメータ（HTTP接続のホスト名とユーザエージェント）を含めることができます。



(注) SCA BBは、すべてのP2Pサービスの分類を100%達成することはできません。これは、永続的に接続を試行するP2Pアプリケーションがあるためです。このようなアプリケーションは、さまざまな代替プロトコルと接続スキームを使用します。ネイティブプロトコルは暗号化され、新しいバージョンがリリースされると、この暗号化はしばしば変更されます。これは、P2Pトラフィックをブロックしようとしても、結果的にはクライアントが接続する場合もあることを意味します。完全にブロックするのではなく、トラフィックの帯域幅を制限し、そのトラフィックを無効にするほうがよい場合もあります。

サービス要素

サービスは1つまたは複数のサービス要素で構成されており、異なるネットワークトラフィックフロータイプが異なるサービス要素にマッピングされています。

サービス要素は特定のプロトコル、開始側、ゾーン、およびフレバを、選択されたサービスに対応付けます。これらのパラメータの一部または全部にワイルドカードが使用できます。



(注)

単方向分類が有効になっている場合、サービス要素のフレーバは常にワイルドカード値となります。

次の4つの基準をすべて満たすトラフィックフローが特定のサービスにマッピングされます。

- フローがサービス要素の指定のプロトコルを使用している。
- フローの開始側が、サービス要素で指定された開始側と一致する。
- フローの宛先が、サービス要素の指定ゾーンに属するアドレスである。
- フローが、サービス要素の指定のフレーバと一致している。

フローが2つのサービス要素と一致し、一方が他方よりも詳細であれば、このフローはより詳細なサービス要素にマッピングされます。

たとえば、サービスAにブラウジングが定義され、サービスBに特定のURLリストのブラウジングが定義されているとします。サービスBのリストにあるURLのブラウジングフローは、どちらのサービスとも一致しますが、この場合はサービスBにマッピングされます。

任意のサービス要素の任意のパラメータに一致するフローが別の要素の別のパラメータにも一致する場合、一致するパラメータの優先順位はフレーバが最も高く、次がプロトコル、その次がゾーン、最後が開始側となります。

たとえば、サービスAにEメールが、サービスBに指定されたネットワークゾーンのすべてのトラフィックが定義されているとします。指定されたネットワークゾーンのEメールフローは、どちらのサービスとも一致しますが、この場合はサービスAにマッピングされます。

サービスの例

表 3-1 に、サービスとそのネットワークパラメータの例を示します。

表 3-1 サービスおよびサービスパラメータの例

サービス名	プロトコル	開始側	ゾーン	フレーバ
Web ブラウジング	HTTP HTTPS	サブスクライバ側	—	—
Web ホスティング (ネットワーク側開始ブラウジング)	HTTP HTTPS	ネットワーク側	—	—
ローカル SMTP	Simple Mail Transfer Protocol (SMTP; シンプルメール転送プロトコル)	—	ローカルメールサーバ (215.53.64.0/24)	—

プロトコル

フローの主な分類の1つにセッションのプロトコル（セッションを開始したネットワークアプリケーションのプロトコル）があります。

SCA BB システムで定義されているように、プロトコルは1つまたは複数のシグニチャ、1つまたは複数のポート番号、および転送タイプの組み合わせで構成されています。ネットワークフローのプロトコルはこれらのパラメータに従って識別されます。たとえばポート番号が80、転送タイプがTCPであり、コンテンツがHTTPシグニチャと一致する場合、SCA BBはこのフローをHTTPプロトコルにマッピングします。

デフォルトのサービスコンフィギュレーションには、事前に定義されたプロトコルのリストがあります。プロトコルは追加できます。

TCPまたはUDPフローが特定のプロトコル定義に一致しない場合、SCA BBはこのフローをGeneric TCPまたはGeneric UDPプロトコルにマッピングします。

非TCPまたは非UDPフローが特定のプロトコル定義に一致しない場合、SCA BBはこのフローをGeneric IPプロトコルにマッピングします。

単方向分類が有効になっている場合、プロトコル分類は、単方向UDPフローを除いて、通常の方法で実行されます。この場合、SCA BBは最初のパケットの宛先ポートを使用して分類しようとします。完全に一致するものが見つからなければ、SCA BBは送信元ポートを使用してプロトコル进行分类しようとします。

プロトコル要素

プロトコルは、プロトコル要素の集合です。

プロトコル要素は特定のシグニチャ、IPプロトコル、およびポート範囲を、選択されたプロトコルに対応付けます。パラメータにはワイルドカードを含めることができ、ポート番号を範囲で指定することもできます。

次の3つの基準をすべて満たすトラフィックフローが特定のプロトコルにマッピングされます。

- フローのシグニチャがプロトコル要素で指定されたシグニチャと一致する。
- フローのプロトコルがプロトコル要素のIPプロトコルと一致する。
- フローのポート範囲がプロトコル要素で指定されたポート範囲と一致する。
- フローが2つのプロトコル要素に一致し、一方が他方よりも詳細であれば、フローはより詳細なプロトコル要素にマッピングされる。

たとえば、プロトコルAがFTPシグニチャと一致するフローに定義され、プロトコルBがTCPポート21のFTPシグニチャと一致するフローに定義されているとします。ポート21のFTPフローは、どちらのプロトコルとも一致しますが、この場合はプロトコルBにマッピングされます。

- フローが、あるプロトコル要素のシグニチャと別のプロトコル要素のポートのどちらにも一致する場合、そのフローはシグニチャと一致するプロトコルにマッピングされる。

たとえば、プロトコルAがFTPシグニチャと一致するフローに定義され、プロトコルBがTCPポート21のフローに定義されているとします。ポート21のFTPフローは、どちらのプロトコルとも一致しますが、この場合はプロトコルAにマッピングされます。

ポートベース プロトコルの簡単な定義方法

特定ポートのすべての汎用（分類されていない）トラフィックは、<「Generic」シグニチャ, 特定ポート>という形式のプロトコル要素をプロトコルに追加することで、そのプロトコルに割り当てることができます。特定ポートの「Generic」シグニチャがプロトコルに割り当てられると、「Behavioral」シグニチャも自動的にそのプロトコルに割り当てられます。たとえばデフォルトコンフィギュレーションでは、ポート555の「Generic」シグニチャはH20プロトコルに割り当てられるので、ポート555の「Behavioral Upload/Download」シグニチャも自動的にH20プロトコルに割り当てられます。

この割り当ては自動的に実行されるため、ユーザは手動で割り当てを行う必要はありません。自動的に追加されるこれらのプロトコル要素は、GUIには表示されません。一方、ユーザが特定ポートの「Behavioral Upload/Download」シグニチャを別のプロトコルに割り当てするには、適切なプロトコル要素を作成し、それを別のプロトコルに割り当てます。



(注)

デフォルト コンフィギュレーションでは、プロトコル要素 <「Generic」シグニチャ, 特定ポート 80> を含めることで、HTTP プロトコル定義は HTTP シグニチャだけでなく、ポート 80 のその他の汎用（分類されていない）トラフィックもすべて受け入れます。前述したように、<「Generic」シグニチャ, 特定ポート> 形式のプロトコル要素が特定のプロトコル定義に使用されている場合、SCE はその特定ポートの Generic および Behavioral シグニチャの両方をそのプロトコルにマッピングします。

HTTP の場合は、「Behavioral Upload/Download」シグニチャとして分類されているポート 80 のトラフィックもその HTTP プロトコルに割り当てられます。ここまで述べてきたように、この動作の目的はポートベース プロトコルを簡単に定義することです。ただし、プロトコル要素 <「Behavioral」シグニチャ, 特定ポート> を他のプロトコルに追加すると、この動作を回避できます。

シグニチャ

SCA BB は、SCE プラットフォームの緻密なパケット検査機能でトラフィック フローを検査し、それぞれのフローとインストールされたプロトコル シグニチャのセットを比較して、フローを生成したネットワーク アプリケーションを特定します。

SCA BB には、一般的なネットワーク アプリケーションの定義済みシグニチャとプロトコルのセットが用意されています。たとえば、ブラウジング、E メール、ファイル共有、VoIP などです。

単方向分類が有効になっている場合、SCE プラットフォームを単方向フロー（インバウンドまたはアウトバウンド）が通過すると、そのフローは単方向プロトコル シグニチャの特定セットと照合されます。双方向フローが SCE プラットフォームを通過する場合、プロトコル ライブラリはそのフローを標準の（双方向）プロトコル シグニチャの 1 つと照合します。

シスコは新しいシグニチャを含むプロトコル パックを定期的に発行して、シグニチャをアップデートしています。これらのプロトコル パックを使用して SCA BB にインストールされたシグニチャのセットをアップデートすれば分類機能を強化できます。

ダイナミック シグニチャ

SCA BB が使用するシグニチャのほとんどは定義済みであり、ハードコード化されています。また、ユーザがダイナミック シグニチャを追加して独自に定義することもできます。

ダイナミック シグニチャは、Signature Editor ツールで作成および編集ができます。SCA BB の Dynamic Signature Script (DSS) エンジンでは、定義されたシグニチャのほかにこれらのユーザ定義シグニチャを使って分類を行います。

開始側

通常、SCE プラットフォームはプロバイダーのサブスクリバとネットワークの間に配置されます。サブスクリバ側で開始されたフローはサブスクリバからネットワークに伝送され、ネットワーク側で開始されたフローはネットワークからサブスクリバに伝送されます。

フロータイプによっては開始側を制限することができます。たとえば、HTTP フローの開始側をサブスクリバに制限できます。HTTP が開始されるのはサブスクリバがインターネットを利用するときなので、常にサブスクリバ側から開始されるからです。HTTP フローがネットワーク側から開始される場合は、サブスクリバのローカル マシン上で Web サーバがオープンになっており、着信 HTTP トラフィックを受信していると考えられます。プロバイダーはネットワーク側から開始される HTTP をブロックできます。

ゾーン

ゾーンは、ネットワーク側の IP アドレスの集合です。

共通の目的で接続されているグループごとに IP アドレスを割り振ることによってゾーンを設定できます。サブスクリイバのネットワーク フローがサービスにマッピングされて、ゾーンに適用されることもあります。実際は、ゾーンには地理的な領域が定義されることがほとんどです。

ゾーンはネットワーク セッションを分類するために使用します。ネットワーク セッションは、宛先 IP アドレスに基づいてサービス要素に割り当てられます。

ゾーンの例

- 「囲いのある庭」: プレミアム ビデオ コンテンツを持つサーバ ファームの IP アドレス範囲。プロバイダーは特定のサブスクリイバへのアクセスを制限し、トラフィックの優先順位を確保します。
- オフネットとオンネットのフローを区別するためのゾーン。

ゾーンをセッションに割り当てる例

- ゾーン A とゾーン B はいずれもユーザが定義したゾーンであり、ゾーン A の IP アドレスは 10.1.0.0/16、ゾーン B の IP アドレスは 10.2.0.0/16 であるとします。新しいセッションのネットワーク IP アドレスが 10.1.1.1 の場合、このセッションはゾーン A のセッションとなります。

ゾーン項目

ゾーンは、関連するゾーン項目の集合です。

ゾーン項目は、1 つの IP アドレスまたは IP アドレスの範囲です。

表 3-2 にゾーン項目の例を示します。

表 3-2 ゾーン項目の例

ネットワーク アドレス	例
IP アドレス	123.123.3.2
IP アドレス範囲 (およびマスク)	123.3.123.0/24 IP アドレスの最初の 24 ビットは指定通りであり、最後の 8 ビットは任意の値となります (すべての IP アドレスが 123.3.123.0 ~ 123.3.123.255 になります)。

フレーバ

フレーバは、ネットワーク セッションをシグニチャ固有のレイヤ 7 プロパティに基づいて詳細に分類するための要素です。

フレーバは、Service Control ソリューションのサービスをさらに細かく定義します。プロトコル フレーバは、サービスを分類する場合にプロトコル属性を追加し、このサービスをプロトコルだけに基づくサービスのフレーバにします。たとえば、HTTP プロトコルのユーザ エージェント属性をプロトコル フレーバとして追加すると、同じブラウザ タイプで生成されたすべての HTTP トラフィックの定義を 1 つのサービスにすることができます。ブラウザ タイプはユーザ エージェント フィールドで確認できます。

フレーバ タイプの例には、HTTP ユーザ エージェントや、Session Initiation Protocol (SIP) ソース ドメインがあります。



(注)

単方向分類が有効になっている場合、フレールバはトラフィックの分類には使用されません。

フレールバ項目

フレールバは、フレールバ項目の集合です。

フレールバ項目のタイプはフレールバタイプによって異なります。使用できるフレールバタイプのリストは、「[フレールバタイプとパラメータ](#)」(P.7-48)を参照してください。

デフォルトのサービスコンフィギュレーションは、HTTP Streaming Agent (HTTP のフレールバ) や Vonage (SIP のフレールバ) などのように事前に定義されたフレールバです。

DSCP ToS

フレールバタイプのひとつに Type of Service (ToS) があります。このタイプでは、Differentiated Service Code Point (DSCP; Diffserv コードポイント) ToS を分類基準として使用できるので、特定のマーキングを伝送するパケットを、無制限の帯域幅やレポートなどが設定された定義済みサービスに割り当てることができます。DSCP ToS 分類プロセスは、他の分類メカニズムよりも優先されます。これにより、音声ゲートウェイなどの外部デバイスが、フローの処理方法を指示できます。DSCP ToS ベースの分類は、独自の管理サービスをマーキングするためのすぐれた方法です。SCA BB はアプリケーションを認識しませんが、DSCP ToS フィールドによってそれらを識別します。

コンテンツフィルタリング

コンテンツフィルタリングでは、要求された URL に従って、HTTP フローの分類と制御を行います。URL の分類は、外部データベースにアクセスして行われます。

サービスプロバイダーは、訴訟を回避したり保護者による管理ができるなど、サブスクライバにとって効果的な Web フィルタリングを必要としています。ここで問題になるのは、Web は大規模なうえに成長を続けている一方で、SCA BB や SCE プラットフォームは効果的なフィルタリングを必要とする巨大な URL データベースを追跡、管理するようには設計されていない点です。

そこで、SCA BB は、SurfControl Content Portal Authority (CPA) に統合された、コンテンツフィルタリングを提供します。SurfControl の技術により、ネットワーク管理者は URL データベースを管理したりサーバと通信することなく SCA BB の URL 分類機能を強化し、強力なフィルタリングソリューションを構築することができます。Web でのアクセスが非常に多いサイトや、性的な表現、人種差別、ハッカーなどリスクカテゴリ別に分類された URL のデータベースへのアクセスを、関連分野も含めて完全に網羅することができます。

SurfControl の CPA を SCA BB に統合することで、必要な Web フィルタリングソリューションが提供されます。SCA BB は SCE プラットフォーム上で実行され、CPA サーバに接続してサブスクライバが要求する Web サイトをカテゴリ化します。カテゴリは HTTP フローを分類するために使用され、この分類は、通常の SCA BB トラフィック制御とレポートに使用されます。



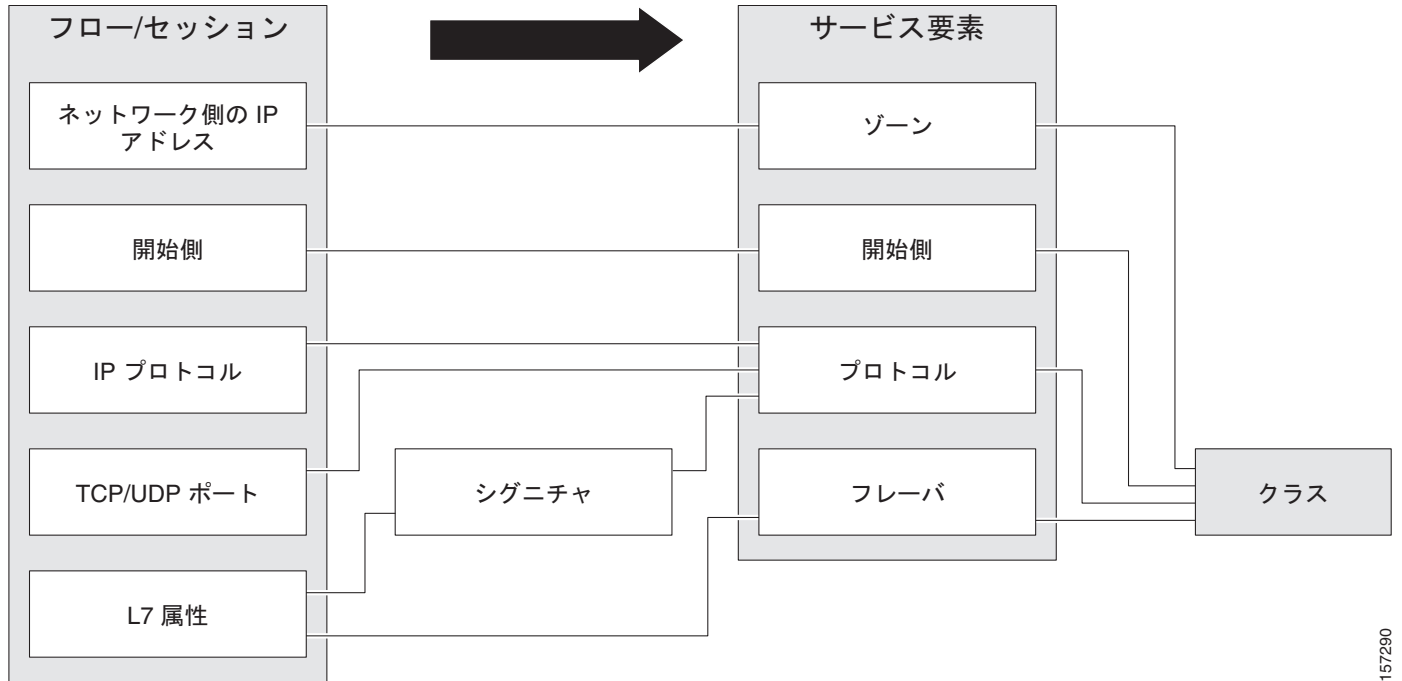
(注)

SCA BB には、HTTP URL フレールバ分類で使用される URL の内部データベースが含まれます。内部データベースと外部のコンテンツフィルタリングデータベースの両方で検出された URL は、内部データベースに従って分類されます。

サービスへのフロー属性のマッピング

図 3-1 は、セッションのフロー要素をサービスのサービス要素にマッピングする場合を示しています。

図 3-1 サービスへのフロー属性のマッピング



157290

トラフィックのアカウントティングとレポート

SCE プラットフォームが収集したデータは、リアルタイム シグナリング、課金、レポートに使用できます。

ユーザ定義の使用カウンタに基づいて、さまざまなメトリックが異なるスコープで収集されます。グローバル（全リンク単位）、サービス単位（またはサービスグループ単位）、パッケージ単位（またはパッケージグループ単位）、サブスライバ単位があります。

- グローバル制御帯域幅はレイヤ 1 のボリュームに基づいています。
- サブスライバ帯域幅制御（およびアカウントティング、レポート）は、レイヤ 3 ボリュームに基づいています。

使用カウンタの値にはプッシュ型とプル型があります。

- SCE プラットフォームは、フローや使用状況などのデータを含む RDR を生成し、伝送します。
- SCE プラットフォームは、外部システムが問い合わせる Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) MIB を保守します。

従量制課金

SCA BB は、さまざまなスコープのネットワーク メトリックをサービス単位で収集し、保守します。次のネットワーク メトリックがあります。

- アップストリームのボリューム (L3 KB)
- ダウンストリームのボリューム (L3 KB)
- セッション
- アクティブなサブスクリイバ
- 並列セッション
- セッション持続時間



(注)

SIP や Media Gateway Control Protocol (MGCP) などの VoIP サービスでは、同時セッション数使用カウンタは同時に行われる音声呼び出しの回数を、セッション持続時間利用使用カウンタは音声呼び出しの持続時間を表します。

サービス単位による課金は次のスコープで発生します。

- サブスクリイバ単位
- サブスクリイバのグループ単位 (パッケージ)
- リンク単位 (グローバル)

複数のサービスが 1 つのサービス使用カウンタを共有することがあります。たとえば、デフォルトのサービス コンフィギュレーションでは、SMTP サービスと Post Office Protocol 3 (POP3) サービスが同じ E メール カウンタを共有します。使用カウンタへのサービスの割り当てはサービス階層によって決まります。サービス階層については次のセクションで説明します。同様に、複数のパッケージが 1 つのパッケージ使用カウンタを共有することもあります。この場合のパッケージと使用カウンタの割り当てはパッケージ階層(「[パッケージ階層](#)」(P.3-11)を参照)によって決まります。

サービス階層

サービスは階層ツリーに配置されます。単一のデフォルト サービスがルートにあり、ツリー内の任意の場所に新しいサービスをそれぞれ配置できます。詳細については、「[サービス](#)」(P.3-2)を参照してください。

サービスは親の規則を継承します。(特定のパッケージ内の) 特定のサービスに規則が定義されている場合は、明示的に指定されていないかぎり、すべての子サービスがそのパッケージの同じ規則によって制御されます。

サービス使用カウンタ

サービス階層を使用すると、サービスをその意味に従って編成するだけでなく、使用カウンタを共有することもできます。サービスはサービス階層が定義したグループに応じて分類されます。各サービスには使用カウンタが割り当てられます。

サービスの使用カウンタには 2 つのカテゴリがあります。

- グローバル : Link Usage RDR、Package Usage RDR、およびレポートに使用されます。
- サブスクリイバ : Real-Time Subscriber Usage RDR およびレポートに使用されます。

サービスごとにグローバル使用カウンタおよびサブスクリバ使用カウンタが1つずつ割り当てられます。特定のサービスに分類されたトラフィックだけのサービス使用量をカウントしたり、親サービスのトラフィックと併せてカウントすることができます。たとえば、「Premium Video Content」というサービスが「Streaming」の子として定義されている場合、オペレータは Premium Video Content 専用の使用カウンタを定義したり、「Streaming」と同じ使用カウンタを使うように設定することができます。グローバル使用カウンタとサブスクリバ使用カウンタは独立しています。サービスが同じ場合、一方の使用カウンタの親と子が同じでも他方の使用カウンタは子だけが同じということもあります。

パッケージ階層

パッケージは階層ツリーに配置されます。単一のデフォルトパッケージがルートにあり、ツリー内の任意の場所に新しいパッケージをそれぞれ配置できます。詳細については、「[パッケージ](#)」(P.3-13)を参照してください。

パッケージ使用カウンタ

パッケージ階層を使用すると、パッケージはその意味に従って編成され、パッケージ使用カウンタが共有されます。サービス コンフィギュレーションごとに最大 1024 個のパッケージ使用カウンタを定義して、そのうちの1つを Unknown Subscriber Traffic パッケージに使用できます。

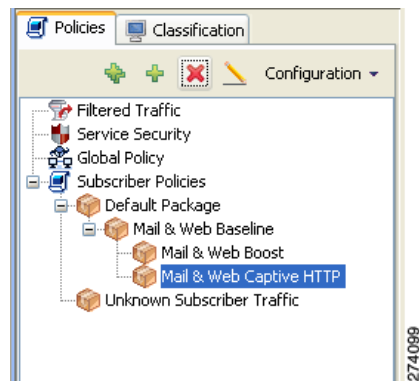
パッケージ レベルでの使用量レポートは、次のようにグループ化されます。

- 専用の使用カウンタが割り当てられたパッケージ：このパッケージに対応付けられたすべてのトラフィックは、割り当てられたカウンタで個別にカウントされます。その場合、専用カウンタが割り当てられていないすべての子も一緒にカウントされます。
- 専用のパッケージ使用カウンタが割り当てられていないパッケージ：このパッケージに対応付けられたすべてのトラフィックは、親パッケージと一緒にカウントされます。

図 3-2 に、パッケージ ツリーの例を示します。この例では、Mail & Web Baseline パッケージに専用カウンタが割り当てられていて、子パッケージに専用カウンタが割り当てられていない場合、すべての Package Usage RDR および派生レポート（「Package Bandwidth per Service」など）は、3 つのすべてのパッケージに割り当てられたサブスクリバの使用量を合計します。

ただし、Mail & Web Boost パッケージにも専用カウンタがある場合は、Main & Web Baseline および Mail & Web Captive HTTP のトラフィックと一緒にカウントされ、Mail & Web Boost のトラフィックは個別にカウントされます（一般的に、これは効率的なコンフィギュレーションではありません。階層構造は同じカウンタが共有できるグループ パッケージに使用すべきです）。

図 3-2 パッケージ ツリーの例



レポート

SCA BB を実行する SCE プラットフォームは、サービス プロバイダーに関する情報が格納された RDR を生成して送信します。

RDR には、システム設定に応じてさまざまな情報および統計情報が格納されます。

RDR は、シスコ独自仕様のプロトコルを使用して送信されます。したがって、Cisco Service Control Management Suite (SCMS) Collection Manager (CM) を使用するか、または RDR を処理するソフトウェアを開発する必要があります。

一部の RDR 内のデータは、業界標準となっている NetFlow レポートング プロトコルでもエクスポートできます。NetFlow レポートングを使用すると SCA BB ソリューションを既存のデータ コレクタに簡単に統合できます。

- 「RDR」 (P.3-12)
- 「NetFlow」 (P.3-13)

RDR

RDR の主なカテゴリは次のとおりです。

- Usage RDR : 定期的に生成されます。使用カウンタの状態がサービス単位およびアカウントング スコープ単位で格納されます。Usage RDR には 4 つのタイプがあります。
 - Link Usage RDR : リンク全体のサービス単位でのグローバルな使用状況。
 - Package Usage RDR : サブスクリバ グループごとのサービス単位での使用状況。
 - Subscriber Usage RDR : サブスクリバごとのサービス単位での使用状況。全サブスクリバに生成されます。Cisco Service Control Management Suite (SCMS) Collection Manager (CM) および Cisco Service Control Application (SCA) Reporter は、この RDR を使用して上位サブスクリバ レポートと集約された使用量課金レコードを生成します。
 - Real-Time Subscriber Usage RDR : 選択されたサブスクリバだけについて生成されます。SCMS-CS および SCA Reporter は、この RDR を使用して詳細なサブスクリバ アクティビティ レポートを生成します。
- Transaction RDR : フロー例について生成されます。上位 TCP ポートなどの統計グラフを作成する場合に使用されます。
- Transaction Usage RDR : ユーザ定義フィルタに合わせてフローごとに作成されます。ブラウジング、ストリーミング、音声フローについてレイヤ 7 の詳細情報が格納されます。フローベースの課金に使用されます。
- Real-Time Signaling RDR : フロー開始や終了など特定のネットワーク イベント時に生成されます。外部システムからネットワークへのリアルタイム アクションを許可する場合に使用されます。
- Malicious Traffic RDR : SCE プラットフォームが Distributed Denial of Service (DDoS; 分散型 サービス拒絶) 攻撃などのトラフィック異常を検出した場合に生成されます。これらの RDR は、攻撃や攻撃者を検出し、これらの影響を軽減するために使用されます。

NetFlow

次の情報は、NetFlow プロトコルを使用してエクスポートできます。

- **Usage** : 定期的に生成されます。使用カウンタの状態がサービス単位およびアカウントリング スコープ単位で格納されます。
- **Malicious Traffic** : SCE プラットフォームが DDoS 攻撃などのトラフィック異常を検出した場合に生成されます。

トラフィックの制御

トラフィックの制御は、サービス、サブスクリイバ パッケージ、サブスクリイバ クォータの状態などに応じて、トラフィック フローをブロック、制限、優先する方法を提供します。

- 「[パッケージ](#)」 (P.3-13)
- 「[サブスクリイバが未知のトラフィック](#)」 (P.3-14)
- 「[規則](#)」 (P.3-14)
- 「[帯域幅の管理](#)」 (P.3-14)
- 「[クォータ管理](#)」 (P.3-17)

パッケージ

パッケージは、サブスクリイバ ポリシーを表す規則の集合です。パッケージには、指定したサブスクリイバ グループに配信されるサービスのグループと、それぞれのサービスに対するシステムの動作が定義されています。ネットワーク フローの制限、フローの優先順位に関するガイドライン、フローをレポートする方法が格納されています。

ネットワークの各サブスクリイバには、自分が所属するパッケージへの参照先が示されます。次に、ネットワークの各サブスクリイバがシステムでどのように参照されるかを示します。

1. フローとサービス要素を一致させ、ネットワーク フローとサービスをマッピングする。
2. フローの発信元であるサブスクリイバを、サブスクリイバのネットワーク ID (通常はサブスクリイバの ID アドレス) に従って識別する。
3. サブスクリイバが所属するパッケージを識別する。
4. サブスクリイバのネットワーク フローのサービスに正しい規則を適用する。

もう 1 つの方法について、「[仮想リンク モード](#)」 (P.3-13) で説明します。

仮想リンク モード

通常モードでは、各パッケージに帯域幅コントローラを定義します（「[帯域幅の管理](#)」 (P.3-14) を参照）。仮想リンク モードでは、テンプレート帯域幅コントローラを定義します。サブスクリイバがシステムに入ると、そのサブスクリイバに実際の帯域幅パラメータが割り当てられます。これらのパラメータはサブスクリイバのパッケージと仮想リンクの方向によって決まります。

詳細については、「[クォータの管理](#)」 (P.9-76) を参照してください。

サブスクリバが未知のトラフィック

SCE プラットフォームは、トラフィック フローを処理するサブスクリバを識別しようとします。SCE プラットフォームはトラフィック フローの IP アドレスまたは VLAN を調べて、内部データベース内で、この IP アドレスまたは VLAN タグで識別されるサブスクリバを確認します。このようなサブスクリバがデータベース内にない場合、トラフィック フローは Unknown Subscriber Traffic カテゴリにマッピングされます。

規則

規則とは、特定サービスのネットワーク フローの処理方法を SCE プラットフォームに伝える一連の命令です。次のような規則があります。

- フローの処理を次のように指定する。
 - ブロックする。
 - 一定の帯域幅を割り当てる。
 - そのフローのパケット DSCP ToS を所定の値でマーキングする（「[DSCP ToS マーキング](#)」(P.3-20) を参照）。
- 集約ボリュームまたはセッション制限を定義し、フローに制限を適用する。
- 課金や分析のためにフローをレポートする方法を指定する。

カレンダー

カレンダーを使用して、1 週間を 4 つの時間枠に分割できます。

カレンダーの設定後、そのカレンダーを使用するパッケージに「[タイムベース規則](#)」(P.3-14) を追加できます。

タイムベース規則

タイムベース規則とは、1 つの時間枠だけに適用される規則です。タイムベース規則を使用すると、一定の時間だけに適用される規則パラメータを設定できます。たとえば、ピーク、オフピーク、夜間、週末用にそれぞれ異なる規則を定義する必要がある場合もあるでしょう。

規則には、タイムベース規則を追加できます。時間枠に対してタイムベース規則が定義されていない場合、親規則が適用されます。

異なる時間枠に同様の規則を適用する必要がある場合があります。タイムベース規則を追加するとき、親規則の設定を新しいタイムベース規則にコピーし、必要な変更を行うことができます。親規則に対してそれ以降に行った変更は、タイムベース規則には影響しません。

帯域幅の管理

システムを通過する帯域幅には絶対的な制限があり、これを物理リンク帯域幅と呼びます。SCE プラットフォームを通過する総帯域幅を物理リンクの帯域幅よりも小さい値に制限できます。たとえば、IP ストリーム上で SCE プラットフォームの隣に位置するデバイスの BW 容量が限られている場合、他のデバイスの容量に合わせて、SCE プラットフォームを通過する帯域幅を制限できます。

SCA BB の帯域幅制御には 2 つの段階があります。

- グローバル制御

- サブスライバ帯域幅制御
- グローバル制御帯域幅はレイヤ 1 のボリュームに基づいています。
- サブスライバ帯域幅制御（およびアカウントリング、レポート）は、レイヤ 3 ボリュームに基づいています。

グローバル帯域幅制御

全体の帯域幅使用状況はグローバルコントローラで制御します。グローバルコントローラは、SCEプラットフォームの仮想キューです。グローバルコントローラはシステム全体に設定し、サブスライバごとには設定しません。

グローバルコントローラは、「Total Gold Subscriber Traffic」や「Total P2P Traffic」などといった大容量のグローバルなトラフィックを制限します。各グローバルコントローラは、特定のタイプのすべてのトラフィックに割り当てられる利用可能な合計帯域幅の最大割合を定義します。グローバルコントローラを使用すると、P2Pなどのシステム内のサービスの合計トラフィックを利用可能な合計帯域幅の指定した割合に制限できます。このようにして、このトラフィックで消費する合計帯域幅を管理できます。

デフォルトでは、アップストリームインターフェイスとダウンストリームインターフェイスには、リンクトラフィックを100%制御する、デフォルトグローバルコントローラが1つずつ割り当てられています。各インターフェイスには最大1023のグローバルコントローラを追加できます。また、各グローバルコントローラには合計リンク制限の最大割合を個別に割り当てることができます。

各グローバルコントローラには、利用可能な合計帯域の最大割合の値をタイムフレームごとに個別に定義できます（「カレンダー」(P.3-14)を参照）。

デュアルリンクシステムでは、各リンクに異なる帯域幅の値を定義できます。また、2つのリンクを通過する集約帯域幅を制限することもできます。

仮想リンクモードでは、テンプレートグローバルコントローラが使用されます。テンプレートグローバルコントローラは、仮想キューのテンプレートであり、システム内と同数の個別物理リンクに適用されます。それぞれの物理リンクの実際の帯域幅パラメータは、リンクによって異なります（詳細については、「クォータの管理」(P.9-76)を参照してください）。

サブスライバ帯域幅制御

個別のサブスライバが使用する帯域幅は、サブスライバ BW Controller (BWC; BW コントローラ) で制御します。それぞれの BWC は、指定したサービスで利用できる帯域幅を制御します。特定の BWC が制御するサービスはパッケージごとに定義されますが、帯域幅制御はサービスごとに設定します。

BWC は次のパラメータで指定されます。

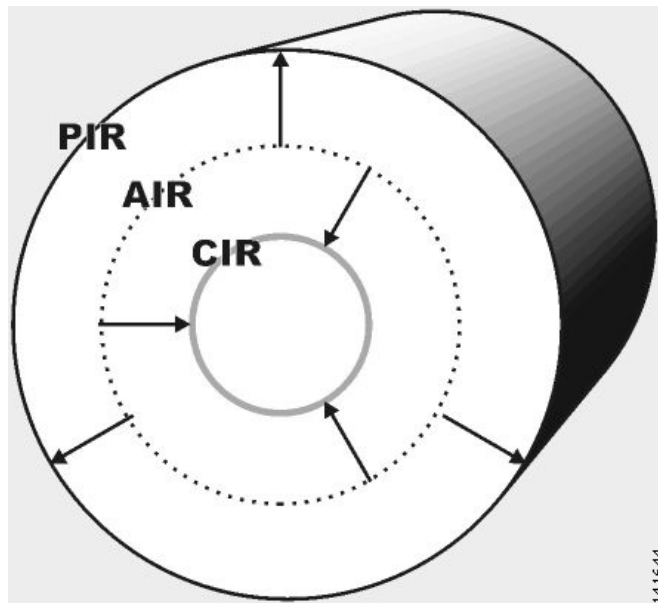
- [Committed Information Rate (CIR)] : BWC が制御するサービスに割り当てられる最小帯域幅
- [Peak Information Rate (PIR)] : BWC が制御するサービスに割り当てられる最大帯域幅
- [Global Controller] : この BWC のリンク先グローバルコントローラ
- [Assurance Level (AL)] : トラフィック輻輳時に利用可能な帯域幅が変化するレート

図 3-3 に示すように、利用可能な最大帯域幅 (Admitted Information Rate (AIR)) は CIR から PIR までの範囲になります。実際に消費される帯域幅は、常に AIR 未満です。

BWC には、さまざまな輻輳条件で AIR の判別方法を制御する 3 番目のパラメータがあります。システムは、ネットワークが輻輳していない場合は PIR を、ネットワークの輻輳が激しい場合は CIR を実現します。これらの 2 つの極端な状態の間では、AIR は 3 番目のパラメータ [Assurance Level (AL)] によって決定されます。AL は、輻輳増加時に AIR が PIR から CIR に低下する速度を、輻輳緩和時に AIR が CIR から PIR に増大する速度を制御します。AL が小さい場合よりも、AL の値が大きい方が、AIR が大きくなります。

BWC は、ネットワークが輻輳していても (PIR 輻輳)、最低限 CIR が保証されるようにします。同様に、BWC は、BWC に関連付けられているトラフィックがほとんどなくても、PIR を超えないように保証します。

図 3-3 帯域幅制御レベル



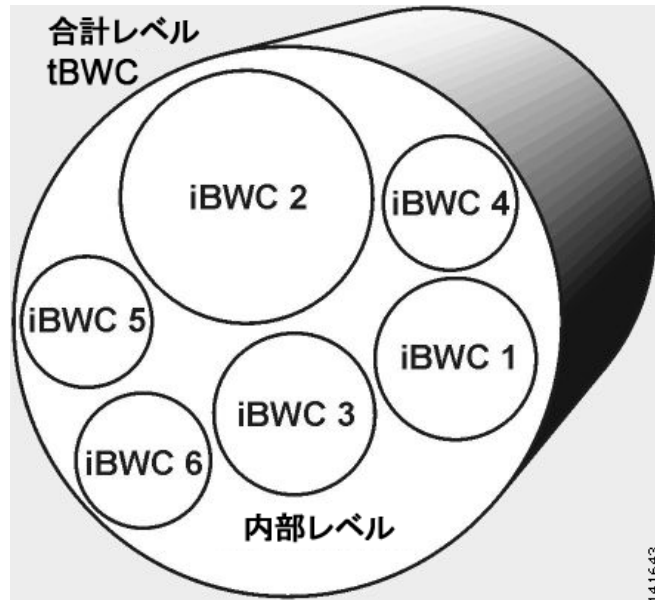
帯域幅は、調整可能な幅の仮想パイプとして考えることもできます。PIR は仮想パイプの最大許容幅です。CIR はこのパイプが収縮する際の最小幅です。AIR は、このパイプの実際の幅です。ネットワークの輻輳時は、システムは各パイプを個別に縮小して、サブスクリバ間およびサービス間で差別化します。

プライマリと内部の帯域幅の制御

図 3-4 に示すように、SCA BB では、各サブスクリバに独立した BWC セットがあります。この BWC セットは、そのサブスクリバに使用可能な総帯域幅を制御する単一のプライマリ (合計) BWC (tBWC) と、そのサブスクリバの一部のサービスに使用できる帯域幅を制御するいくつかの内部 BWC (iBWC) で構成されています。たとえば、ある BWC がストリーミングサービスを制御し、別の BWC がダウンロードと E メールサービスをまとめて制御する場合があります。

関連付けられているサービスの最大帯域幅は PIR によって、最小帯域幅は CIR によって定義されます。

図 3-4 2つのレベルの帯域幅制御



iBWC は次の方法でトラフィックにリンクできます。

1. パッケージ全般を定義する場合は、1つのサブスライバ BWC を追加して、その CIR、PIR、AL、および CoS によって定義します。
2. 規則を定義する場合は、各サービスを1つのサブスライバ BWC に割り当てます。

クォータ管理

指定したサービスのクォータ制限をサブスライバに割り当てることができます。

各サブスライバには 16 のクォータ バケットがあり、バケットごとにボリュームやセッションが定義できます。サブスライバが特定のサービスを使用すると、使用したボリュームやセッション数の総計がいずれかのバケットから差し引かれます。

各サービスで使用するバケットはサービス コンフィギュレーションで指定します。ボリューム バケットの消費量は、L3 KB で測定します。セッション バケットの消費量はセッション数で測定します。たとえば、ブラウジングと E メール サービスをバケット #1 のクォータで消費し、P2P サービスをバケット #2 のクォータで消費し、その他のサービスはいずれも特定のバケットにバインドされないように定義することができます。

外部クォータ プロビジョニング システムでクォータ プロビジョニング API を使って、各バケットのクォータを動的に変更することができます。クォータ プロビジョニング API については、『Cisco SCMS SCE Subscriber API Programmer's Guide』を参照してください。たとえば、サブスライバがクォータを追加購入した場合は特定のバケットのクォータを増やすことができます。これらの外部システムから各バケットのクォータの残量を問い合わせることもできます。この方法を使用すると、たとえば、サブスライバ個人の Web ページにクォータの残量を表示させることができます。

外部クォータ プロビジョニングは、Quota Manager (QM) を使って取得することもできます。QM はシスコが提供するソリューションです。QM のインストールおよび動作の詳細については、『Cisco Service Control Management Suite Quota Manager User Guide』を参照してください。

外部クォータ プロビジョニングは、Gy クォータ モデルを使って取得することもできます。詳細については、『Cisco Service Control Mobile Solution Guide』を参照してください。



(注) 単方向分類が有効になっている場合、外部クォータ プロビジョニングはサポートされません。

内部 SCA BB クォータ プロビジョニング システムは、各クォータ バケットの容量が一定となるように一定の間隔で補充します。

バケットのクォータが使用できなくなった場合はサブスクリバに通知されます。

サブスクリバ通知

サブスクリバ通知機能を使用すると、サブスクリバ HTTP トラフィックを該当する Web ページにリダイレクトさせ、Web ベースのメッセージ (クォータの枯渇など) をサブスクリバに送信させることができます。HTTP のリダイレクションは、サブスクリバ通知がアクティブになると開始し、サブスクリバ通知が解除されると終了します。



(注) 単方向分類が有効になっている場合、サブスクリバ通知はサポートされません。

その他のトラフィック処理機能

このセクションでは、SCA BB のその他トラフィック処理機能について説明します。

- 「サービス セキュリティ」 (P.3-18)
- 「トラフィック フィルタ」 (P.3-20)
- 「Value Added Services サーバへのトラフィック フォワーディング」 (P.3-20)

サービス セキュリティ

SCA BB にはサービス セキュリティ機能が用意されており、ネットワーク オペレータやサブスクリバを次のような攻撃や悪質なトラフィックから保護します。

- Denial of Service (DoS; サービス拒絶) 攻撃
- DDoS 攻撃
- VoIP 脅威
- ワーム
- ハッカーの活動
- サブスクリバ コンピュータが悪質な乗っ取りに遭うこと
 - スпам ゾンビ
 - E メール ベースのウイルス

Service Control ソリューションを使用してもネットワークの脅威から完全に保護することは不可能ですが、ネットワーク内での悪質な活動を見抜き、ネットワーク全体のパフォーマンスを損なわないように広範囲にわたる悪質な活動を抑えることはできます。

ネットワーク オペレータは SCA BB で次のことが実行できます。

- 疑わしい動きのあるネットワーク トラフィックを監視する。
- 悪質なトラフィックをブロックする。

- 悪質なトラフィックを発生させているサブスクリバ、または影響を受けているサブスクリバに通知する。

悪質なトラフィックの検出

SCA BB には 3 つの脅威検出メカニズムがあります。

- 異常検出：ホスト IP アドレス同士の接続速度（成功した場合も失敗した場合も）をモニタします。接続速度が速い場合、または接続の成否の比率が低い場合は悪質なアクティビティであることを示します。

異常検出機能により、次のカテゴリのアクティビティであることがわかります。

- IP スウィープ：同一ポート上の複数の IP アドレスをスキャン（ワームの典型的な行動）
- ポート スキャン：1 つの IP アドレスの全ポートをスキャン（ハッカーの典型的な行動）
- DoS 攻撃：1 つの IP アドレスから 1 つの IP アドレスへの攻撃
- DDoS 攻撃：複数の IP アドレスから 1 つの IP アドレスへの攻撃



(注)

SCA BB は、スプーフィングを行う DoS 攻撃を DDoS 攻撃と認識します（本物ではなく偽の IP アドレスが多数使用されます）。

- 異常検出メカニズムは、新しい脅威の出現に対応する場合に効果的です。脅威の本質やレイヤ 7 シグニチャについて知る必要がなく、ネットワーク アクティビティの特性に基づいているからです。
- 大量のメール配信の検出：個別のサブスクリバの SNMP セッション比率をモニタします（SCE プラットフォーム サブスクリバ アウェアネスを使用します。サブスクリバ アウェア モードまたはアノニマス サブスクリバ モードで動作するからです）。単一サブスクリバからの SMTP セッション レートが高いということは、E メール送信に関連する悪質なアクティビティを一般的に示します（E メールベースのウイルスまたはスパムゾンビ アクティビティ）。
- シグニチャ ベースの検出：SCE プラットフォームのステートフル レイヤ 7 機能を使用して、他のメカニズムでは検出が難しい悪質なアクティビティを検出します。オペレータはこのような脅威のシグニチャを追加し、新しい脅威に素早く反応することができます。

悪質なトラフィックへの応答

前のセクションで説明した検出メカニズムを設定する場合は、次の対策を実行します。

- これらのメカニズムで検出された悪質なアクティビティについてネットワークをモニタする。悪質なアクティビティ分析で収集したデータのグラフを Console に表示できます。
- SCE プラットフォームによって検出された悪質なアクティビティを自動的にブロックし、ネットワークに脅威が広まって悪影響が出るのを防ぐ。
- サブスクリバの Web セッションを専用ポータルにリダイレクトし、悪質なアクティビティの被害に遭っていることを知らせる。

SCA BB には高度な柔軟性があり、検出メソッドを調整して悪質なアクティビティを定義したり、悪質なアクティビティが検出された場合の対策を設定することができます。

トラフィック フィルタ

フィルタ規則はサービス コンフィギュレーションの一部です。フィルタ規則を指定すると、SCE プラットフォームに一部のフロー タイプ（フローのレイヤ 3 およびレイヤ 4 プロパティによる）を無視させ、フローを変更なしで伝送させることができます。

トラフィック フローが SCE プラットフォームに着信すると、SCE プラットフォームはこのフローにフィルタ規則が適用できるかどうかを調べます。このトラフィック フローにフィルタ規則を適用する場合、SCE プラットフォームは次の処理のいずれかを実行します。

- **バイパス**：SCE プラットフォームはトラフィック フローを伝送キューに渡します。このとき RDR は生成されず（分析を目的として生成されたレコードにはこのフローは含まれません）、サービス コンフィギュレーション規則も適用されません。
- **クイック フォワーディング**：遅延に影響されやすいフローの低遅延を保証するためのフロー フィルタ規則動作です。クイック フォワーディングで転送されたフローのパケットは複製され、別のパスを通じて送信されます。複製の一方が直接送信キューに入るので、遅延は最小限にとどまります。もう一方の複製は通常のパケット パスで送信されます。

フィルタ規則では、フィルタ処理されたトラフィックの DSCP ToS 値も設定できます（「[DSCP ToS マーキング](#)」(P.3-20) を参照）。

SCE プラットフォームを通過する Operational Support System (OSS; オペレーション サポート システム) プロトコル (Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) など)、およびルーティング プロトコル (Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) など) にフィルタ規則を追加することを推奨します。このようなプロトコルは一般的にポリシーの実施から影響を受けず、ボリュームが少ないので、レポートする必要性はあまりありません。

デフォルト サービス コンフィギュレーションには多数のフィルタ規則が用意されています。

特定プロトコルのフローを、そのフローのレイヤ 7 特性に基づいてフィルタリングすることもできます。

DSCP ToS マーキング

DSCP ToS マーキングは、ネットワーク要素間のフローのタイプとプライオリティを通知するために IP ネットワークで使用されます。DSCP ToS マーキングは、通常はネットワークでのトラフィックの処理方法を認識している要素によって実行されます。こうした要素は、音声ゲートウェイなどトラフィックを生成する要素の場合もあります。たとえばアプリケーション アウェアである SCA BB は、ビジネス モデルや、遅延に影響されやすいアプリケーション固有のニーズに基づいて、帯域幅リソースを割り当てることができます。

Value Added Services サーバへのトラフィック フォワーディング

Value Added Services (VAS) サーバへのトラフィック フォワーディング機能を利用すると、Service Control ソリューションで外部エキスパート システム (VAS サーバ) を使ってトラフィック処理を追加できます。SCE は事前設定された VAS サーバのロケーションにトラフィックを再ルーティングします。処理後はトラフィックが SCE に戻され、本来の宛先に送信されます。



(注)

単方向分類が有効になっている場合、VAS トラフィック フォワーディングはサポートされません。

サービス コンフィギュレーション

サービス コンフィギュレーションは、プロバイダーのビジネス戦略と展望を実現し強化します。

サービス コンフィギュレーションは、該当する SCE プラットフォームに伝播されて初めて有効になります。サービス コンフィギュレーションは、SCA BB を通過するネットワーク トラフィックを分析することで強化されます。

サービス コンフィギュレーションの構成は次のとおりです。

- トラフィック分類の設定：Web ブラウジングなどのサービス、ファイル共有、および VoIP。それぞれのサービスは、ネットワーク トラフィックとサービスのマッピング方法を定義する要素で構成されています。サービスのコンフィギュレーション構築ブロックは、プロトコル、ゾーン、フレーバ、シグニチャです。
- トラフィックのアカウントティングとレポートの設定：トラフィック フローおよびネットワークの従量制課金をレポートする方法に関する設定。
- トラフィック制御の設定：サービス別に定義された一連の規則（帯域幅レート制限やクォータ制限など）で構成されたパッケージ。パッケージの主なコンフィギュレーション構築ブロックは、規則、クォータ バケット、サブスライバ BWC、グローバル コントローラです。

サービス コンフィギュレーション定義の実際

実際のサービス コンフィギュレーション定義は繰り返し処理です。

次の手順を推奨します。

1. システムをセットアップします。
2. デフォルトのサービス コンフィギュレーションを適用します。
3. データを収集します。
4. 分析します。
5. 次のいずれかまたは両方を実行します。
 - トラフィックをさらにサービスに分割してトラフィックを検出する。
 - サービスおよびサブスライバのパッケージに基づいてトラフィックの制限や優先順位の規則を作成する。

