CHAPTER 10

# Service Configuration Editor の使用法：その他のオプション

この章では、Service Configuration Editor で使用できるその他の詳細機能の使用法について説明します。

# サービス セキュリティ ダッシュボード

サービス セキュリティ ダッシュボードでは、すべての SCA BB セキュリティ機能を表示して制御できます。

サービス セキュリティ ダッシュボードは、ワーム、DDoS 攻撃、スパム ゾンビなどのセキュリティの脅威からネットワークを保護する機能へのゲートウェイです。検出メカニズム（攻撃のしきい値など）、および攻撃が検出されたときに実行する処理を設定できます。

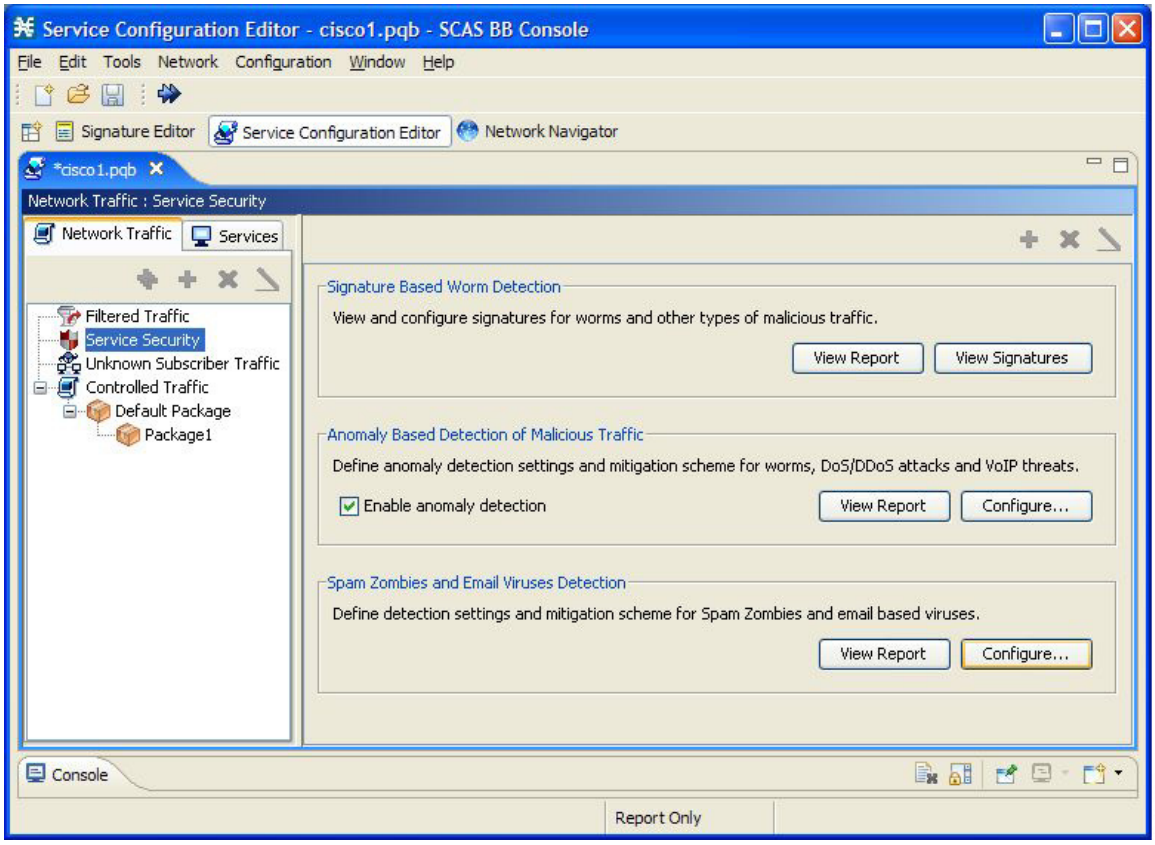
サービス セキュリティ ダッシュボードでは、Reporter ツールの悪質トラフィック レポートにアクセスすることもできます。

## サービス セキュリティ ダッシュボードの表示

**ステップ 1**　Network Traffic タブで **Service Security** を選択します。

**ステップ 2**　サービス セキュリティ ダッシュボードが右側ペインに表示されます。

**図 10-1**




さまざまな検出メカニズムの表示と設定、および悪質トラフィック レポートの表示については、次のセクションで説明します。

## ワーム検出

SCA BB では、ワームの検出に次の 3 つのメカニズムが使用されます。

- シグニチャ ベース検出 — Service Control Engine（SCE）プラットフォームのステートフル レイヤ 7 機能では、その他のメカニズムで容易に検出できない悪質アクティビティを検出できます。新しいワームのシグニチャを追加できます。
- 異常ベース検出 — 全体的なトラフィック分析により、ワーム アクティビティを示すことがある異常を検出できます。「異常検出の管理」（p.10-3）を参照してください。
- 大量メール送信ベース検出 — 電子メール トラフィック分析により、電子メールベース ワームを示すことがある異常を検出できます。「スパム検出の設定」（p.10-16）を参照してください。

### サポートされるワーム シグニチャの表示

**ステップ 1**　サービス セキュリティ ダッシュボードで **View Signatures** をクリックします。

Signature Type ドロップダウン リストから Worm Signatures が選択された状態で Signatures Settings ダイアログボックスが表示されます。

サポートされているすべてのワーム シグニチャがリストされます。

**ステップ 2**　**Close** をクリックします。

Signature Settings ダイアログボックスが閉じます。

### サービス コンフィギュレーションへの新規ワーム シグニチャの追加

次のうちいずれかを実行します。

**ステップ 1**　シスコが提供する最新 DSS ファイルまたは SPQI ファイルをインポートします。

**ステップ 2**　サービス コンフィギュレーションに追加するワーム シグニチャを含む DSS ファイルを作成します。

## 関連情報

詳細情報については、「プロトコル シグニチャの管理」（p.7-39）を参照してください。

## 異常検出の管理

最も総合的な脅威検出方式は異常検出です。

異常検出の基本原理は、システムが確認するすべての IP アドレスとの正常接続レート（TCP の場合は正しい確立、その他のプロトコルの場合は双方向）と異常接続レート（TCP の場合は不正な確立、その他のプロトコルの場合は単一方向）を監視すること、および次の基準のうちいずれかに基づく異常検出条件をトリガーすることです。

- 合計接続レートが定義済みしきい値を超える。
- 不審接続レートが定義済みしきい値を超え、かつ不審接続と非不審接続の比率が定義済みしきい値を超える。

比率メトリックは特に強力な悪質アクティビティ インジケータであり、信頼できる悪質アクティビティ識別子としてレート修飾子とともに動作します。

異常検出は、検出された異常条件の方向に基づいて、次の 3 つのカテゴリに分類されます。3 つのカテゴリで使用されるコンセプトは同じですが、検出される悪質アクティビティの性質はカテゴリごとに異なります。

- スキャンおよびスウィープ ディテクタ — IP アドレスからの接続レートにおける異常に基づく悪質アクティビティを検出します。
- DoS ディテクタ — IP アドレスのペア間における接続レートの異常を検出します。一方が他方を攻撃している IP アドレスのペア間において、接続レートで異常を検出します。単一の攻撃またはスケールが大きい DDoS 攻撃の一部である可能性があります。
- DDoS ディテクタ — IP アドレスに着信する接続レートで異常を検出します（その IP アドレスが攻撃されている）。攻撃は、単一 IP アドレス（DoS）または複数の IP アドレスによって行われる可能性があります。

すべての種類の異常検出条件において、次のそれぞれにしきい値および実行されるトリガー処理を定義できるので、柔軟性が最大になります。

- フロー方向
- フロー プロトコル
- （オプション）TCP および UDP のポートの一意性

**（注）** ここで説明する GUI 設定は、前リリースで使用できた、SCE プラットフォームの攻撃フィルタリング モジュールを設定する CLI コマンドの代わりとなります。

## 異常検出パラメータ

スキャンおよびスウィープ、DoS、DDoS という異常ディテクタ カテゴリごとに、1 つのデフォルト ディテクタがあります。カテゴリごとに別のディテクタを追加できます。各カテゴリのディテクタは順番に確認されます。ディテクタのしきい値設定に従った最初の一致によって検出がトリガーされます。ディテクタが確認される順序を設定できますが、デフォルト ディテクタは最後に確認されます。

異常ディテクタには、悪質トラフィックに関連する、最大 12 の異常タイプを含めることができます。

- ネットワーク主導 — ネットワーク側から開始される悪質トラフィック
  - TCP — すべてのポートの集約 TCP トラフィック
  - TCP 特定ポート — すべての単一ポートの TCP トラフィック
  - UDP — すべてのポートの集約 UDP トラフィック
  - UDP 特定ポート — すべての単一ポートの UDP トラフィック
  - ICMP — すべてのポートの集約 ICMP トラフィック
  - その他 — すべてのポートでその他のプロトコル タイプを使用した集約トラフィック
- サブスクライバ主導 — サブスクライバ側から開始される悪質トラフィック
  - TCP
  - TCP 特定ポート

- UDP
- UDP 特定ポート
- ICMP
- その他

（注）　DoS 攻撃ディテクタでは、ICMP およびその他の異常タイプを使用できません。

ディテクタの各異常タイプには次のアトリビュートが関連します。

- 検出しきい値 — 2 つのしきい値があり、どちらかを超えるということは、攻撃が進行中であると定義されることになります。
  - セッション レートしきい値 — 異常検出条件をトリガーする、単一 IP アドレスの指定ポートにおける 1 秒間のセッション数
  - 不審セッションしきい値　—　不審セッションとは、適切に確立されていないセッション（TCP の場合）、または単一方向セッション（その他のプロトコルの場合）のことです。不審セッション レートおよび不審セッション比率の両方を超えると、異常検出条件がトリガーされます。セッション レートが比較的高くて応答レートが低い場合は、一般的に悪質アクティビティを示します。
  - 不審セッション レート — 単一 IP アドレスの指定ポートにおける、1 秒間の不審セッション数
  - 不審セッション比率 — 不審セッション レートと合計セッション レートの比率（パーセンテージ）。比率が高い場合は多くのセッションが応答を受けないことを意味し、悪質アクティビティを示します。
- 処理 — 異常検出条件がトリガーされたとき、次の処理のうち 0 個以上を実行できます（デフォルトでは処理が有効になっていません）。

（注）　デバイス上のログ ファイルに異常をログすること、および RDR の生成を異常タイプごとに設定することはできません。

- ユーザ警告 — SNMP トラップを生成し（シスコ固有の MIB については、『*Cisco Service Control Application for Broadband Reference Guide*』の「SCA BB Proprietary MIB Reference」の章を参照）、異常の始まりと終わりを示します。
- サブスクライバ通知 — ブラウジング セッションをキャプティブ ポータルにリダイレクトし、悪質アクティビティについて関連サブスクライバに通知します。ネットワーク攻撃に関するサブスクライバ通知を設定するには、「サブスクライバ通知の管理」（p.10-27）を参照してください。
- 攻撃ブロック　— 関連セッションをブロックします。ブロックは、異常検出条件をトリガーした悪質トラフィックの仕様に基づいて実行されます。サブスクライバ通知を異常タイプで有効にしている場合、ブロックはブラウジングの関連ポート（デフォルトの場合は TCP ポート 80。「詳細サービス コンフィギュレーション オプションの管理」[p.10-40] を参照）に適用されません。

ユーザ定義ディテクタにも、次のアトリビュートのうち 1 つ以上を含めることができます。

- IP アドレス リスト — リストされている IP アドレス範囲に検出を制限します。IP スウィープおよびポート スキャンの検出時に、送信元 IP に適用されます。DoS 攻撃および DDoS 攻撃の検出時には送信先 IP に適用されます。
- TCP ポート リスト — リストされている送信先 TCP ポートに検出を制限します。このリストは、TCP 指定ポート異常タイプのみに適用されます。

- UDP ポート リスト — リストされている送信先 UDP ポートに検出を制限します。このリストは、UDP 指定ポート異常タイプのみに適用されます。

## 異常検出設定の表示

すべての異常検出のリストを表示できます。異常ディテクタはツリー構造で表示され、ディテクタカテゴリ（スキャンおよびスウィープ、DoS、DDoS）に従ってグループ化されます。

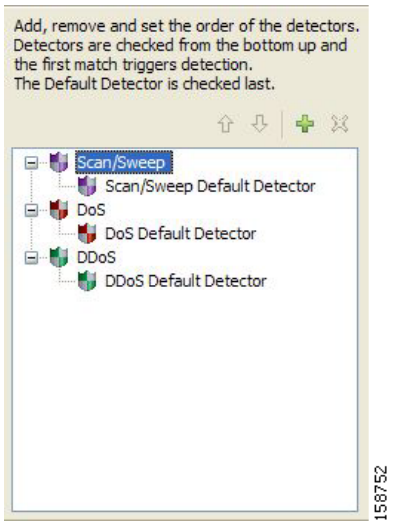
異常ディテクタごとに関連パラメータを表示し、ディテクタに組み込まれるすべての異常タイプのリスト、およびそのパラメータを表示できます。

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

ディテクタ ツリーがダイアログボックスの左側領域に表示され、右側領域は空になります。

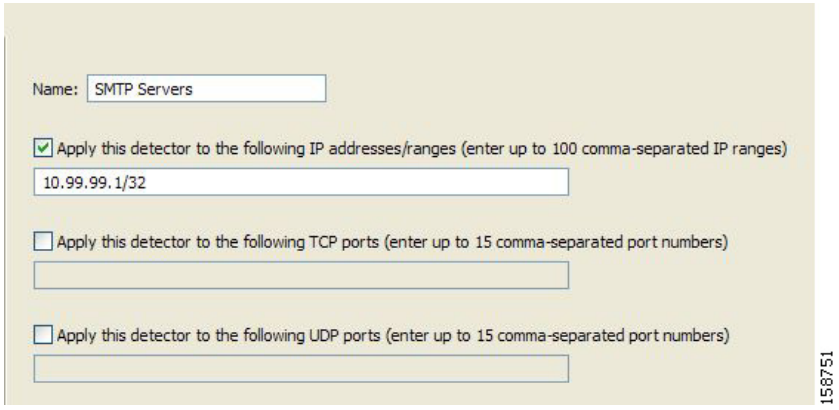
**図 10-2**




**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

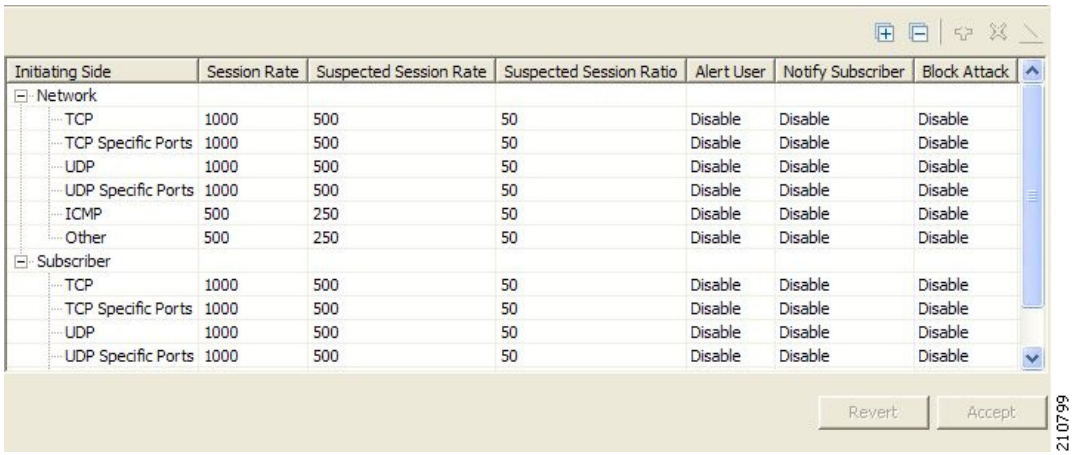
ディテクタのパラメータがダイアログボックスの右上の領域に表示されます。

**図 10-3**




ディテクタの定義済み異常タイプは、各パラメータの値とともにダイアログボックスの右下の領域にリスト表示されます。次の図は、スキャンおよびスウィープのデフォルト ディテクタのデフォルト パラメータ値を示しています。

**図 10-4**




非対称ルーティング分類モードがイネーブルになっている場合、不審セッション レートとセッション レートは同じに設定されます。この設定では、不審セッションによりトリガーされる異常検出が実質的にディセーブルになります。

**ステップ 3**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

## 異常ディテクタの追加

新しい異常ディテクタを追加できます。サービス コンフィギュレーションには 100 までの異常ディテクタを含めることができます。

新しいディテクタには、IP アドレス範囲、TCP ポートと UDP ポート、1 つの異常タイプを定義します。

ディテクタを定義したら、別の異常タイプを追加できます（「異常ディテクタの編集」[p.10-11] を参照）。

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

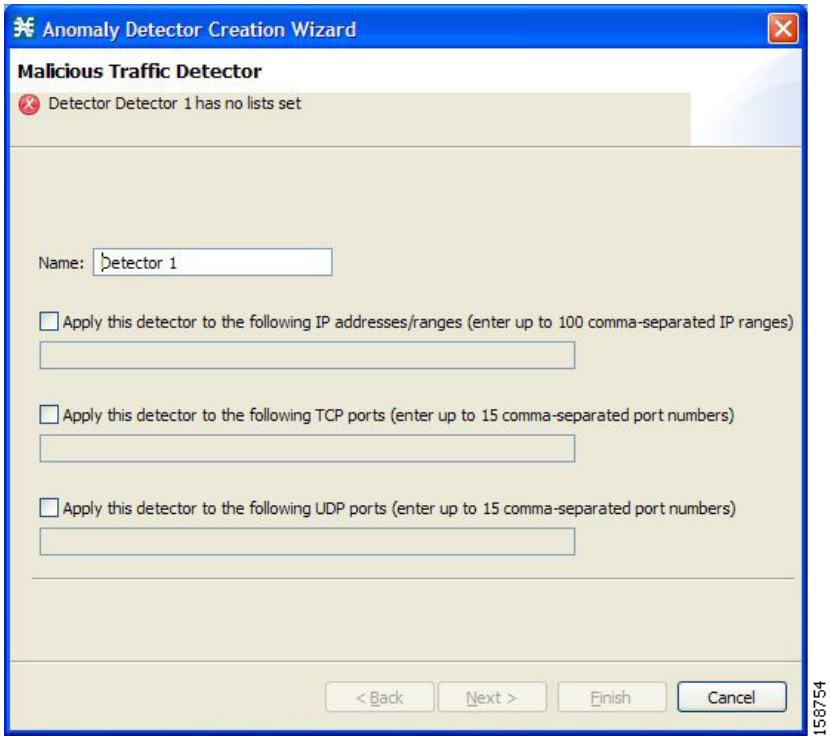
Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタ カテゴリを選択します。

**ステップ 3**　 をクリックします。

Anomaly Detector Creation ウィザードが表示され、Malicious Traffic Detector 画面が開きます。

**図 10-5**




**ステップ 4**　ディテクタのわかりやすい名前を Name フィールドに入力します。

**ステップ 5**　1 つ以上のチェック ボックスをオンにして、ディテクタの範囲を制限します。

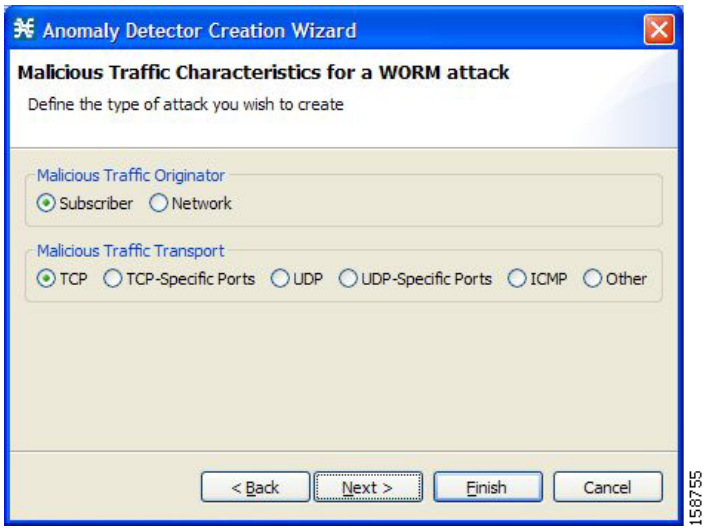
関連フィールドが有効になります。

**ステップ 6**　IP アドレスやポートのリストを関連フィールドに入力します。

**ステップ 7**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Malicious Traffic Characteristics for a WORM attack 画面が開きます。

**図 10-6**




**ステップ 8**　スキャンおよびスウィープ ディテクタまたは DoS ディテクタを定義している場合は、定義している異常タイプの発信側を選択します。

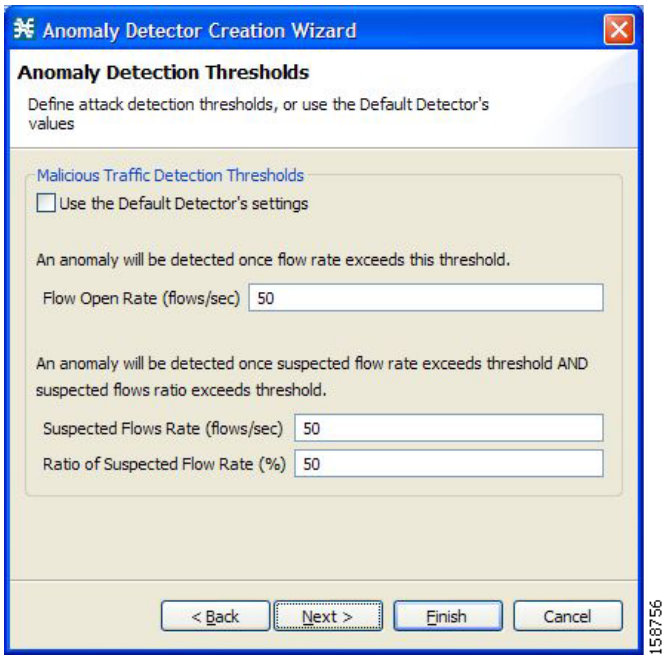
DDoS ディテクタを定義している場合は、定義している異常タイプのターゲット側を選択します。

**ステップ 9**　定義している異常タイプのトランスポート タイプを選択します。

**ステップ 10**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Anomaly Detection Thresholds 画面が開きます。

**図 10-7**



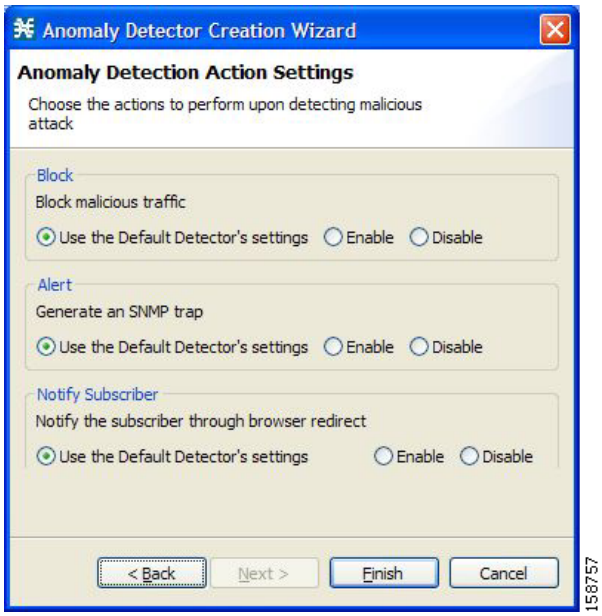

**ステップ 11**　次のうちいずれかを実行します。

- この異常タイプにデフォルト ディテクタの設定を使用するには、**Use the Default Detector's settings** チェック ボックスをオンにします。
- Flow Open Rate フィールド、Suspected Flows Rate フィールド、Ratio of Suspected Flow Rate フィールドに値を入力します。

**ステップ 12**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Anomaly Detection Action Settings 画面が開きます。

**図 10-8**




**ステップ 13**　Block、Alert、Notify Subscriber のアクションを選択します。

**ステップ 14**　**Finish** をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

新しいディテクタがディテクタ ツリーに追加されます。

**ステップ 15**　別の異常タイプをディテクタに追加できます（「異常ディテクタの編集」[p.10-11] を参照）。

## 異常ディテクタの編集

ユーザ定義異常ディテクタでは、次の処理を実行できます。

- ディテクタ パラメータの編集
- 異常タイプの編集
- 異常タイプの追加
- 異常タイプの削除
- ディテクタ ツリーにおけるディテクタの順序の変更

  ディテクタ カテゴリごとに、ディテクタはディテクタ ツリーにリストされている順序で下から上に確認され、デフォルト ディテクタは最後に確認されます。

3 つのデフォルト ディテクタでは異常タイプを編集できます。

### ディテクタ パラメータの編集

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

ディテクタのパラメータがダイアログボックスの右上の領域に表示されます。

**ステップ 3**　ディテクタの新しい名前を Name フィールドに入力します。

**ステップ 4**　IP アドレス範囲およびポートのチェック ボックスのオンまたはオフを行います。

**ステップ 5**　IP アドレスやポートのリストの入力または修正を関連フィールドで行います。

**ステップ 6**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

変更が保存されます。

### 異常タイプの編集

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

異常タイプに関する情報がダイアログボックスの右下に表示されます。

**ステップ 3**　異常タイプをダブルクリックします。

Anomaly Detector Creation ウィザードが表示され、Anomaly Detection Thresholds 画面が開きます（「異常タイプの追加」[p.10-13] を参照）。

**ステップ 4**　次のうちいずれかを実行します。

- この異常タイプにデフォルト ディテクタの設定を使用するには、**Use the Default Detector's settings** チェック ボックスをオンにします。
- Flow Open Rate フィールド、Suspected Flows Rate フィールド、Ratio of Suspected Flow Rate フィールドの値を変更します。

**ステップ 5**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Anomaly Detection Action Settings 画面が開きます。

**ステップ 6**　Block、Alert、Notify Subscriber のアクションを変更します。

**ステップ 7**　**Finish** をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

異常タイプが変更で更新されます。

**ステップ 8**　ステップ 3 ～ 7、またはステップ 2 ～ 7 をその他の異常タイプで繰り返します。

**ステップ 9**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

---

### 異常タイプの追加

---

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

異常タイプがダイアログボックスの右下の領域にリスト表示されます。

**ステップ 3**　（**Create New Detector Item Under Detector Items Feature**）をクリックします。

Anomaly Detector Creation ウィザードが表示され、Malicious Traffic Characteristics for a WORM attack 画面が開きます（「異常ディテクタの追加」[p.10-8] を参照）。

**ステップ 4**　定義している異常タイプの発信元を選択します。

**ステップ 5**　定義している異常タイプのトランスポート タイプを選択します。

**ステップ 6**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Anomaly Detection Thresholds 画面が開きます。

**ステップ 7**　次のうちいずれかを実行します。

- この異常タイプにデフォルト ディテクタの設定を使用するには、**Use the Default Detector's settings** チェック ボックスをオンにします。
- Flow Open Rate フィールド、Suspected Flows Rate フィールド、Ratio of Suspected Flow Rate フィールドに値を入力します。

**ステップ 8**　**Next** をクリックします。

Anomaly Detector Creation ウィザードの Anomaly Detection Action Settings 画面が開きます。

**ステップ 9**　Block、Alert、Notify Subscriber のアクションを選択します。

**ステップ 10**　**Finish** をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

新しい異常タイプが異常タイプ リストに追加されます。

**ステップ 11**　ステップ 3 ～ 10、またはステップ 2 ～ 10 をその他の異常タイプで繰り返します。

**ステップ 12**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

### 異常タイプの削除

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

異常タイプがダイアログボックスの右下の領域にリスト表示されます。

**ステップ 3**　異常タイプ リストで異常タイプを選択します。

**ステップ 4**　  をクリックします。

選択した異常タイプが異常タイプ リストから削除されます。

**ステップ 5**　ステップ 3 ～ 4、またはステップ 2 ～ 4 をその他の異常タイプで繰り返します。

**ステップ 6**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

### ディテクタが確認される順序の変更

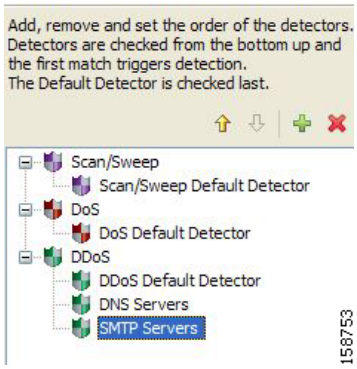
**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーでディテクタを選択します。

ツリーにおけるディテクタの位置により、上矢印か下矢印、またはその両方が有効になります。

**図 10-9**




**ステップ 3**　このナビゲーション矢印を使用し、目的の位置にディテクタを移動します。

**ステップ 4**　ステップ 2 ～ 3 をその他のディテクタに繰り返します。

**ステップ 5**　**OK** をクリックします。

Anomaly Detection Settings ダイアログボックスが閉じます。

変更が保存されます。

## 異常ディテクタの削除

任意のユーザ定義ディテクタまたはすべてのユーザ定義ディテクタを削除できます。

3 つのデフォルト ディテクタは削除できません。

**ステップ 1**　サービス セキュリティ ダッシュボードの Anomaly Based Detection of Malicious Traffic ペインで **Configure** をクリックします。

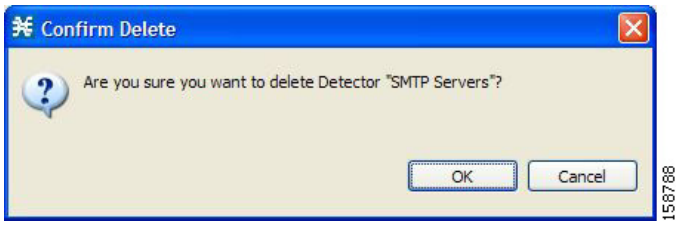
Anomaly Detection Settings ダイアログボックスが表示されます。

**ステップ 2**　ディテクタ ツリーで 1 つ以上のユーザ定義ディテクタを選択します。

**ステップ 3**　をクリックします。

Confirm Delete メッセージが表示されます。

**図 10-10**



**ステップ 4**　**OK** をクリックします。

選択したディテクタが削除され、ディテクタ ツリーに表示されなくなります。

**ステップ 5**　**OK** をクリックします。

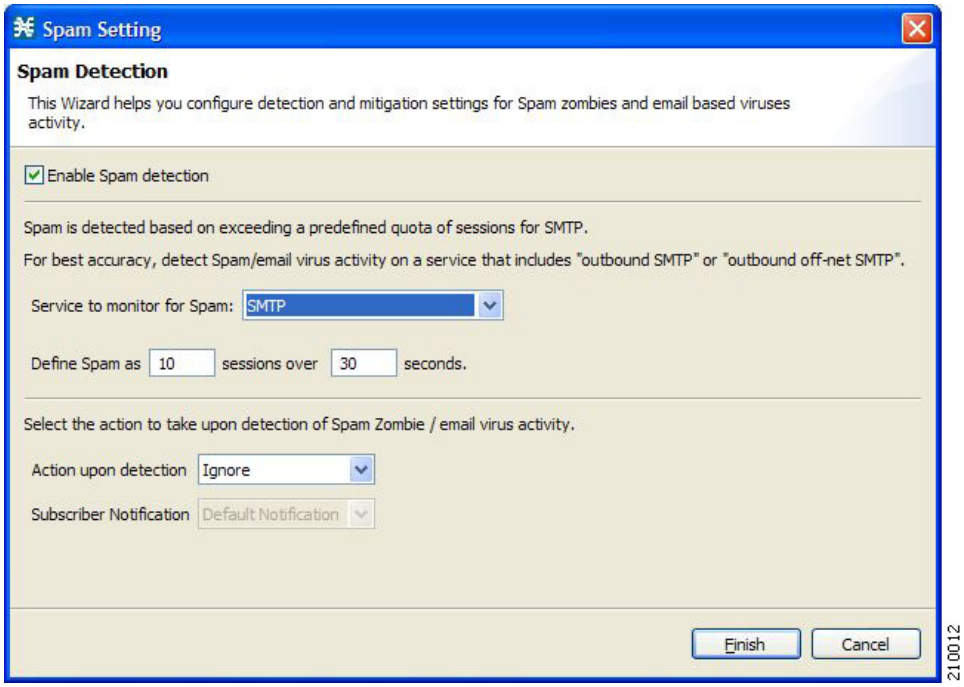
Anomaly Detection Settings ダイアログボックスが閉じます。

## スパム検出の設定

**ステップ 1**　サービス セキュリティ ダッシュボードの Spam Zombies and Email Viruses Detection ペインの **Configure** をクリックします。

Spam Setting ダイアログボックスが表示されます。

**図 10-11**




**ステップ 2**　**Enable Spam detection** チェック ボックスをオフにします。スパム検出が無効になります。

その他すべてのフィールドも無効になります。

ステップ 7 に進んでください。

**ステップ 3**　Service to monitor for Spam ドロップダウン リストからサービスを選択します。

（注）　「発信 SMTP」や「オフネット SMTP」などの限定的なサービスを定義している場合を除いて、監視対象サービス（SMTP）のデフォルト値を変更しないでください。

**ステップ 4**　異常動作の電子メール セッション レートのしきい値を定義します。

**ステップ 5**　悪質アクティビティの検出時に実行する処理を Action upon detection ドロップダウン リストから選択します。

- Ignore（無視）
- Block（ブロック）
- Notify（通知）
- Block and notify（ブロックおよび通知）

**ステップ 6**　Notify または Block and notify を選択すると、Subscriber Notification ドロップダウン リストが有効になります。サブスクライバ通知を選択してください。

（注）　適切なサブスクライバ通知を定義するには、「サブスクライバ通知の管理」（p.10-27）を参照してください。

**ステップ 7**　**Finish** をクリックします。

Spam Setting ダイアログボックスが閉じます。

## 悪質トラフィックに関するレポートの表示についての情報



### 悪質トラフィックに関するレポートの表示

検出されたトラフィック異常に関する情報は Collection Manager（CM）データベースに保存されます。この情報は、ネットワークの傾向調査、新しい脅威の検出、悪質ホストまたはサブスクライバの追跡に使用できます。

Reporter ツールでは、悪質トラフィックに関する多くのレポートを表示できます。

- グローバル レポート
  - Global Scan/Attack Rate
  - Global DoS Rate
  - Infected Subscribers
  - DoS Attacked Subscribers
  - Top Scanned/Attacked ports

- 個別サブスクライバまたはホストのレポート
  - Top Scanning/Attacking hosts
  - Top DoS Attacked hosts
  - Top DoS Attacked Subscribers
  - Top Scanning/Attacking Subscribers

## サービス セキュリティ レポートの表示

**ステップ 1**　サービス セキュリティ ダッシュボードの関連ペインで **View Report** をクリックします。

Choose a report ダイアログボックスが表示され、関連レポートのツリーが表示されます。

**ステップ 2**　レポートのツリーからレポートを選択します。

**ステップ 3**　**OK** をクリックします。

Choose a report ダイアログボックスが閉じます。

Reporter ツールが Console で開き、要求したレポートが表示されます。

**ステップ 4**　レポートの操作方法および保存方法については、『*Cisco Service Control Application Reporter User Guide*』の「Working with Reports」の章を参照してください。

# トラフィック フローのフィルタリング

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。フィルタ規則では、フローのレイヤ 3 プロパティおよびレイヤ 4 プロパティに基づいて一部のフロー タイプを無視し、フローを変更せずに転送するように、Service Control Engine（SCE）プラットフォームに指示できます。

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を適用するかどうかを確認します。

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トラフィック フローを送信キューに渡します。RDR の生成またはサービス コンフィギュレーションの実施は行われません。このフローは、分析用に生成されるレコードに現れず、アクティブなサービス コンフィギュレーションに属す規則によって制御されません。

SCE プラットフォームを通過する OSS プロトコル（DHCP など）、およびルーティング プロトコル（BGP 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。

すべての新しいサービス コンフィギュレーションには、多くのフィルタ規則が組み込まれます。

（注）　デフォルトの場合は、すべてではなく、一部の定義済みフィルタ規則がアクティブになっています。

特定のプロトコルのフローでは、フローのレイヤ 7 の特性によってもフィルタ処理ができます（「詳細サービス コンフィギュレーション オプションの管理」[p.10-40] を参照）。ほかのフィルタ処理されたフローの場合と同様に、レイヤ 7 によるフィルタ処理がされたフローは、分類、制御、レポートが行われません。フィルタ処理可能なプロトコルのフローは一般的に短く、全体のボリュームは無視できます。したがって、これらのプロトコルをフィルタリングしてもネットワーク帯域幅と SCA BB レポートの精度にほとんど影響を与えません。

## パッケージのフィルタ規則の表示

サービス コンフィギュレーションに組み込まれているフィルタ規則のリストを表示できます。

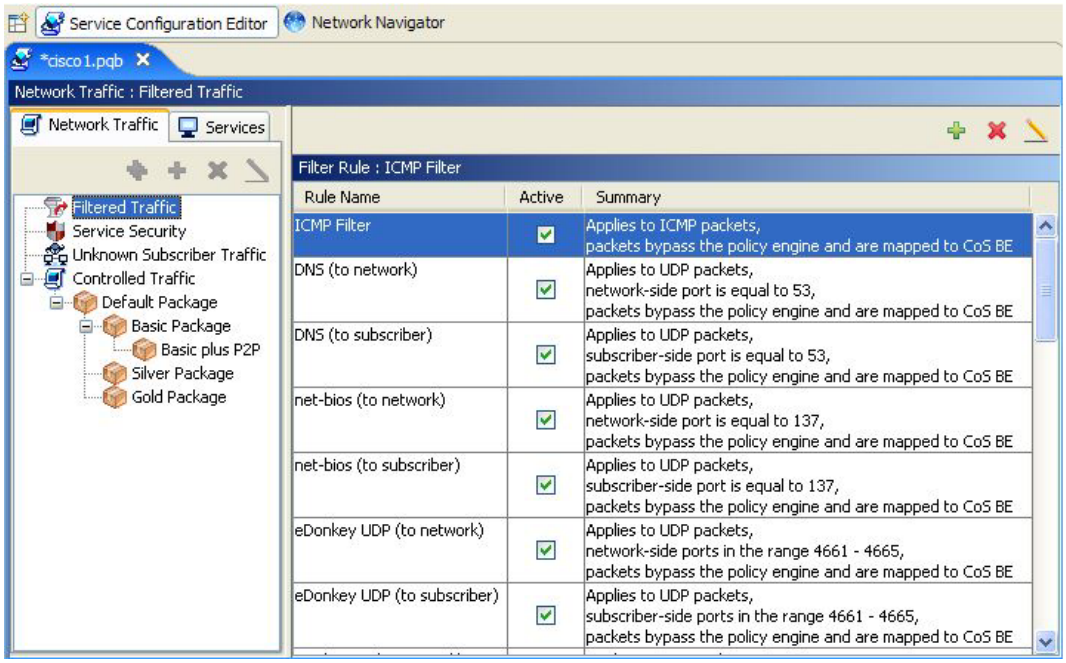
フィルタ規則ごとのリストには、規則の名前、ステータス、簡潔な説明（システムが生成）が含まれます。

フィルタ規則の詳細情報を表示するには、Edit Filter Rule ダイアログボックスを開きます（「フィルタ規則の編集」[p.10-25] を参照）。

**ステップ 1**　Network Traffic タブで **Filtered Traffic** ノードを選択します。

すべてのフィルタ規則のリストが右の規則ペインに表示されます。

**図 10-12**




## フィルタ規則の追加

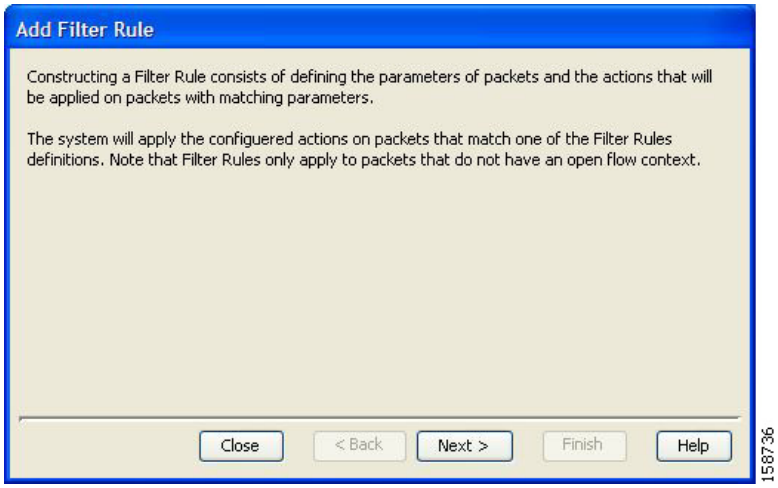
Add Filter Rule ウィザードは、フィルタ規則の追加プロセスを示します。

**ステップ 1**　Network Traffic タブで **Filtered Traffic** ノードを選択します。

**ステップ 2**　右の規則ペインで　（**Add Rules**）をクリックします。

Add Filter Rule ウィザードが表示されます。

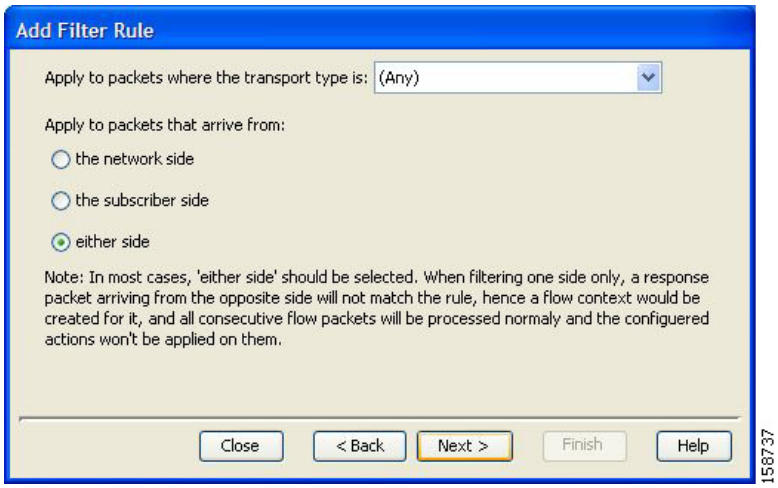
**図 10-13**



**ステップ 3**　**Next** をクリックします。

Add Filter Rule ウィザードの Transport Type and Direction 画面が開きます。

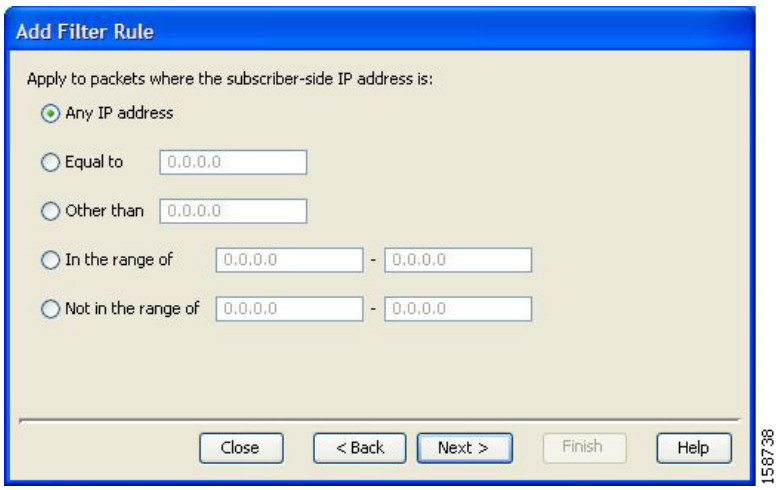
**図 10-14**




**ステップ 4**　トランスポート タイプおよび開始側を選択し、**Next** をクリックします。

Add Filter Rule ウィザードの Subscriber-Side IP Address 画面が開きます。

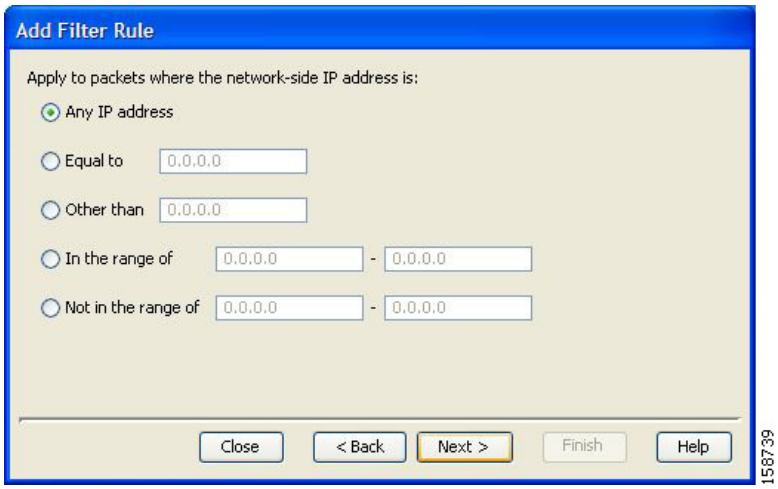
**図 10-15**




**ステップ 5**　サブスクライバ側の IP アドレスを定義し、**Next** をクリックします。

Add Filter Rule ウィザードの Network-Side IP Address 画面が開きます。

**図 10-16**

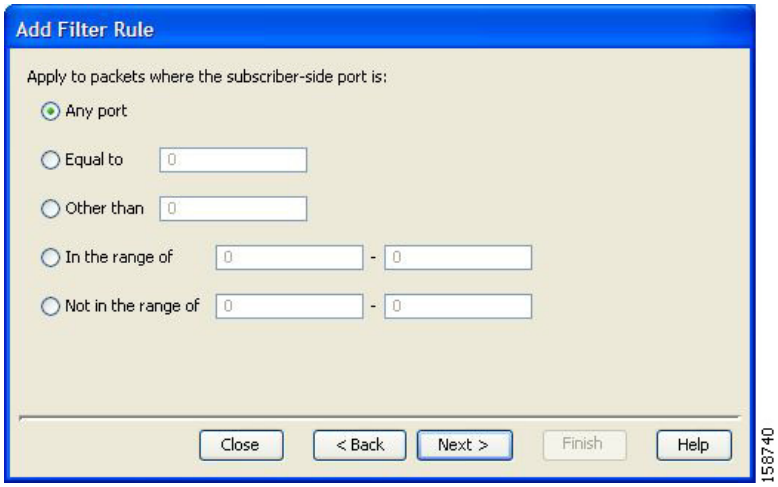



**ステップ 6**　ネットワーク側の IP アドレスを定義し、**Next** をクリックします。

ステップ 4 で選択したトランスポート タイプが TCP か UDP でない場合は、Add Filter Rule ウィザードの ToS 画面が開きます。ステップ 9 に進んでください。

ステップ 4 で選択したトランスポート タイプが TCP か UDP である場合は、Add Filter Rule ウィザードの Subscriber-Side Port 画面が開きます。

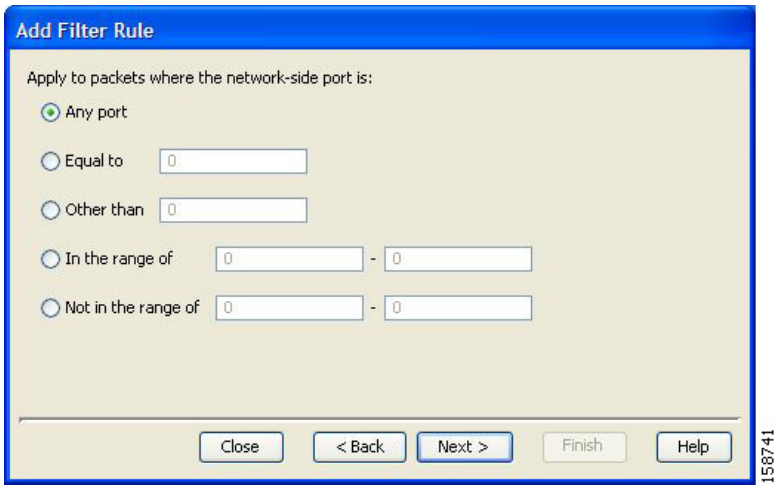
**図 10-17**




**ステップ 7**　サブスクライバ側のポートを定義し、**Next** をクリックします。

Add Filter Rule ウィザードの Network-Side Port 画面が開きます。

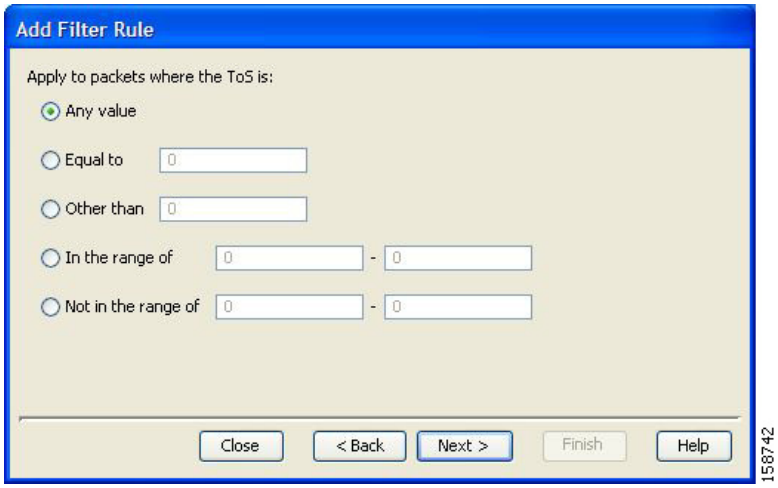
**図 10-18**




**ステップ 8**　ネットワーク側のポートを定義し、**Next** をクリックします。

Add Filter Rule ウィザードの ToS 画面が開きます。

**図 10-19**

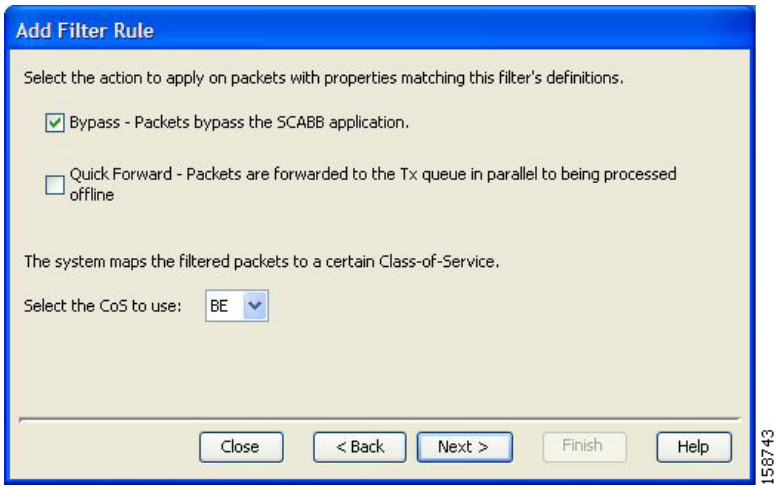



**ステップ 9**　ToS を定義し、**Next** をクリックします。

**（注）**　ToS に指定できる値は 0 ～ 63 です。

Add Filter Rule ウィザードの Action and Class-of-Service 画面が開きます。

**図 10-20**

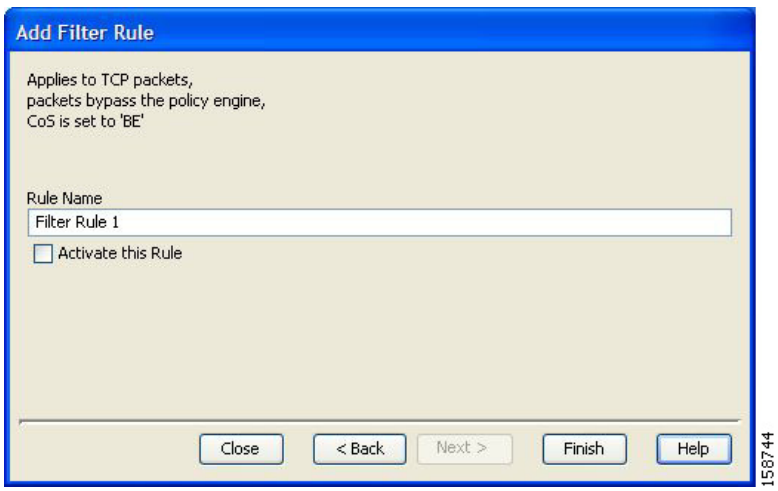



- Bypass — このフィルタ規則に一致するパケットは SCA BB に渡されません。
- Quick Forward — SCE プラットフォームでは、このフィルタ規則に一致するパケットの低遅延が保証されます（遅延に影響されやすいフローに使用）。パケットは複製され、SCA BB に渡されて処理されます。
- Bypass and Quick Forward — SCE プラットフォームでは、このフィルタ規則に一致するパケットの低遅延が保証されます（遅延に影響されやすいフローに使用）。パケットは SCA BB に渡されません。

**ステップ 10**　必要なアクションのオンまたはオフを行い、サービス クラス値を選択して Next をクリックします。

Add Filter Rule ウィザードの Finish 画面が開きます。

**図 10-21**




**ステップ 11**　新しいフィルタ規則の一意の名前を Rule Name フィールドに入力します。

（注）　フィルタ規則にデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

**ステップ 12**　フィルタ規則をアクティブにするには、Activate this rule チェック ボックスをオンにします。トラフィックのフィルタリング基準となるのは、アクティブな規則だけです。

**ステップ 13**　**Finish** をクリックします。

Add Filter Rule ウィザードが閉じます。

フィルタ規則が追加され、Filter Rule テーブルに表示されます。

## フィルタ規則の編集

フィルタ規則のパラメータを表示および編集できます。

**ステップ 1**　Network Traffic タブで Filtered Traffic ノードを選択します。

すべてのフィルタ規則のリストが右の規則ペインに表示されます。

**ステップ 2**　Filter Rule テーブルで規則を選択します。

**ステップ 3**　（**Edit Rule**）をクリックします。

Edit Filter Rule ウィザードの Introduction 画面が表示されます。

Edit Filter Rule ウィザードは Add Filter Rule ウィザードと同じです。

**ステップ 4**　「フィルタ規則の追加」（p.10-20）のステップ 4 ～ 11 の手順に従います。

**ステップ 5**　**Finish** をクリックします。

フィルタ規則が変更され、関連変更内容が Filter Rule テーブルに表示されます。

## フィルタ規則の削除

フィルタ規則を削除できます。サブスクライバ IP アドレスごとに定義された各規則に従って、IP アドレスおよびそのアトリビュートの処理を再開する場合などにフィルタ規則を削除すると便利です。

**ステップ 1**　Network Traffic タブで **Filtered Traffic** ノードを選択します。

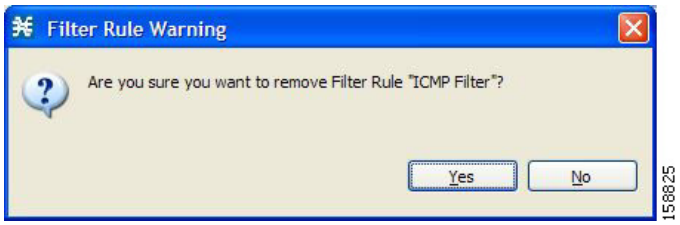
すべてのフィルタ規則のリストが右の規則ペインに表示されます。

**ステップ 2**　Filter Rule テーブルで規則を選択します。

**ステップ 3**　（**Delete Rule**）をクリックします。

フィルタ規則の警告メッセージが表示されます。

**図 10-22**




**ステップ 4**　**Yes** をクリックします。

フィルタ規則が削除され、Filter Rule テーブルに表示されなくなります。

## フィルタ規則の無効化と有効化

フィルタ規則の有効化または無効化はいつでも実行できます。フィルタ規則の無効化にはフィルタ規則の削除と同じ効果がありますが、パラメータはサービス コンフィギュレーションに保持され、あとでフィルタ規則を再び有効にすることができます。

**ステップ 1**　Network Traffic タブで **Filtered Traffic** ノードを選択します。

すべてのフィルタ規則のリストが右の規則ペインに表示されます。

**ステップ 2**　Filter Rule テーブルで規則を選択します。

**ステップ 3**　規則を有効にするには、**Active** チェック ボックスをオンにします。

**ステップ 4**　規則を無効にするには、**Active** チェック ボックスをオフにします。

**ステップ 5**　ステップ 3 ～ 4 をその他の規則に繰り返します。

# サブスクライバ通知の管理

サブスクライバ通知機能では、サブスクライバ HTTP トラフィックが関連 Web ページにリダイレクトされて、Web ベースのメッセージがサブスクライバに示されます。これらの Web ページには、クォータ枯渇の通知など、サブスクライバに関連する情報が含まれています。HTTP のリダイレクションは、サブスクライバ通知がアクティブになると開始し、サブスクライバ通知が解除されると終了します。

（注）　サブスクライバ通知は、非対称ルーティング分類モードではサポートされません。

Cisco Service Control Application for Broadband（SCA BB）では、デフォルト通知およびネットワーク攻撃通知も含めて最大 31 のサブスクライバ通知がサポートされます。



## サブスクライバ通知パラメータ

サブスクライバ通知は次のパラメータで定義します。

- Name — 各サブスクライバ通知には一意の名前を付ける必要があります。

（注）　デフォルト通知またはネットワーク攻撃通知の名前を変更することはできません。

  - Destination URL — リダイレクションを有効にしたあとでサブスクライバの HTTP フローがリダイレクトされる、設定可能な宛先 URL。この Web ページには、通常、サブスクライバに伝達する必要があるメッセージが含まれています。
  - 通知パラメータ — リダイレクション時にオプションとして追加できる宛先 URL のクエリー部分。

  宛先 URL に追加される通知パラメータのフォーマットは、次のとおりです。

- `?n=<notification-ID>&s=<subscriber-ID>`

  <notification-ID> はサブスクライバにリダイレクトされた通知の ID、<subscriber-ID> はサブスクライバ名です。

（注）　「ネットワーク攻撃通知パラメータ」（p.10-29）にはフォーマットが異なるものがあります。

- 宛先 Web サーバではこのパラメータを使用し、意味のあるメッセージをサブスクライバに伝えることができます。
- Dismissal method — 通知状態を解除（非アクティブ）にする時期を指定します。この解除方式は次のいずれかです。

- Subscriber browses to destination URL（デフォルト）— サブスクライバは、宛先 URL をブラウズするとすぐに通知されたとみなされ、通知状態が解除になります。

  たとえば、クォータを超過した場合、サブスクライバが宛先 URL をブラウズするとただちに通知状態が解除され、サブスクライバに通知されます（サブスクライバが引き続き違反状態である場合も同様です）。

- The condition that activated the notification no longer holds — 通知状態の解除は、サブスクライバではなく条件の決定によって決まります。

  たとえば、クォータを超過した場合、通知状態が解除されるのは、サブスクライバが自身のクォータをリフレッシュする手順を完了したときだけです。

（注）　ネットワーク攻撃通知ではこのオプションを使用できません。サブスクライバが通知に対応してから、通知を解除する必要があります。

- Subscriber browses to dismissal URL — サブスクライバが宛先 URL から別の最終 URL に進むまで、通知状態は解除されません。

  サブスクライバが解除 URL にアクセスして通知が解除されるまで、すべての HTTP フローはリダイレクトされます。デフォルトでは、宛先 URL は解除 URL でもあるため、最初のリダイレクションが発生すると、通知が解除されます。ただし、サブスクライバが通知を確認応答するように、別の解除 URL を定義できます。

  たとえば、クォータを超過した場合、宛先 URL にある Web ページで、メッセージを参照したあとに **Acknowledge** ボタンを押すように、サブスクライバに要求することができます。確認応答 URL は解除 URL として定義され、以降の通知は非アクティブになります。

  解除 URL は、URL ホスト名、URL パス、これらを区切るコロンで構成されます。フォーマットは次のとおりです。

- `[*]<hostname>:<path>[*]`
  - <hostname> の前にワイルドカード（*）を付加して、同じサフィックスを持つすべてのホスト名と一致させることができます。
  - パス要素は、常に「/」で開始する必要があります。
  - <path> のあとにワイルドカードを付加して、共通のプレフィックスを持つすべてのパスと一致させることができます。
- たとえば、次のように入力します。
- `*.some-isp.net:/redirect/*`

  この場合は次のすべての URL と一致します。
  - www.some-isp.net/redirect/index.html
  - support.some-isp.net/redirect/info/warning.asp
  - noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8
- List of Allowed URLs — リダイレクションが有効でも、ブロックとリダイレクトが行われない URL のリスト。

  リダイレクションをアクティブにしたあとで、宛先 URL および解除 URL へのフローを除くすべての HTTP フローはブロックされて、宛先 URL にリダイレクトされます。ただし、サブスクライバに追加 URL セットへのアクセスを許可することができます。たとえば、サブスクライバが詳細サポート情報にアクセスできるようにする場合は、これが便利です。

  許可 URL の形式は解除 URL と同じです。

これらのパラメータは、新しいサブスクライバ通知を追加したときに定義されます（「サブスクライバ通知の追加」[p.10-31] を参照）。パラメータの修正はいつでもできます（「サブスクライバ通知の編集」[p.10-32] を参照）。

# ネットワーク攻撃通知についての情報



## ネットワーク攻撃通知

サブスクライバ通知では、サブスクライバにマッピングされた IP アドレスに関連する現在の攻撃について、サブスクライバにリアルタイムで通知されます（これらの通知を有効にする方法は、「サービス セキュリティ ダッシュボード」[p.10-2] を参照してください）。SCA BB は、サブスクライバから送信された HTTP フローを、攻撃に関する情報を提供するサーバへリダイレクトして、攻撃についてサブスクライバに通知します。

サブスクライバ通知の 1 つであるネットワーク攻撃通知はこの通知専用であり、削除できません。ネットワーク攻撃通知は攻撃の最後で解除されず、サブスクライバは応答する必要があります。

トラフィックのブロック時にリダイレクションを許可するには、1 つの指定 TCP ポート（デフォルトではポート 80）を開いておくようにシステムを設定します。「詳細サービス コンフィギュレーション オプションの管理」[p.10-40] を参照してください。

（注）　これまでのバージョンの SCA BB では、CLI コマンドを使用してネットワーク攻撃通知を設定していました。CLI コマンドをこの目的に使用する必要はなくなりました。

## ネットワーク攻撃通知パラメータ

ネットワーク攻撃が検出されると、サブスクライバの HTTP フローは設定可能な宛先 URL にリダイレクトされます。この Web ページでは、サブスクライバに伝達する必要がある警告が表示されます。

宛先 URL には、通知パラメータを含むクエリー部分を含めることもできます。宛先 Web サーバではこのパラメータを使用し、サブスクライバへの特定の警告を作成できます。

宛先 URL のクエリー部分の形式は次のとおりです。

```
?ip=<ip>&side=<side>&dir=<dir>&prot=<protocol>&no=<open-
flows>&nd=<suspected-flows>&to=<open-flows-
threshold>&td=<suspected-flows-
threshold>&ac=<action>&nh=>handled-flows>
```

次の表に、テール内の各フィールドの意味を示します。

表 10-1

| フィールド | 説明 | 指定可能な値 |
|---|---|---|
| ip | 検出された IP アドレス | |
| side | | • s — サブスクライバ<br>• n — ネットワーク |
| dir | | • s — 送信元<br>• d — 宛先 |
| protocol | | • TCP<br>• UDP<br>• ICMP<br>• OTHER |
| open-flows | オープン フロー数 | |
| suspected flows | 攻撃を受けた疑いのあるフロー数 | |
| open-flows-threshold | オープン フローのしきい値 | |
| suspected-flows-threshold | 攻撃を受けた疑いのあるフローのしきい値 | |
| action | | • R — レポート<br>• B — ブロックおよびレポート |
| handled-flows | 攻撃開始以降に処理されたフロー数<br>(攻撃中および攻撃の最後ではゼロ以外) | |

### 説明テールを含む URL の例

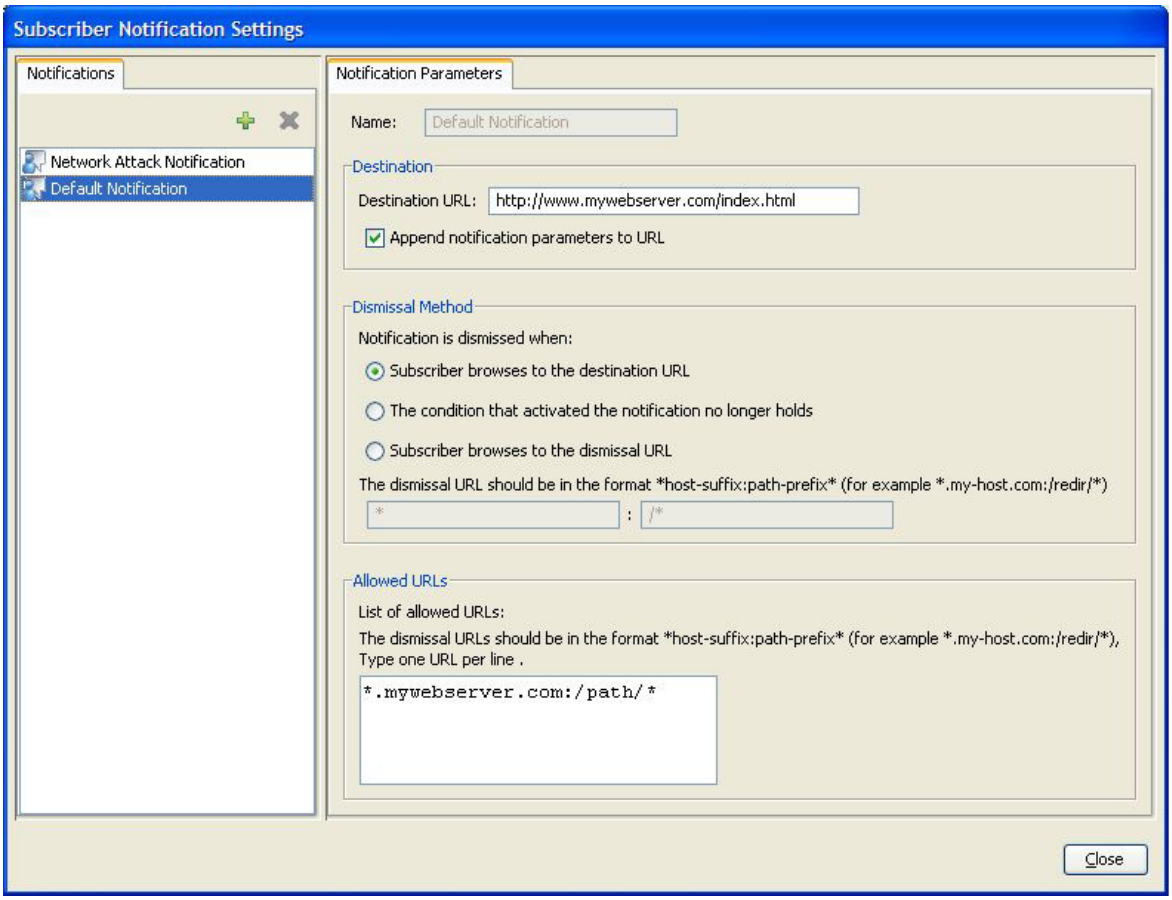
```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&proto=TCP&no=3
4&nd=4&to=34&td=10&ac=B&nh=100
```

## サブスクライバ通知の表示

**ステップ 1**　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

**図 10-23**




すべてのサブスクライバ通知のリストが Notifications タブに表示されます。

**ステップ 2**　パラメータを表示するサブスクライバ通知をリストからクリックします。

サブスクライバ通知のパラメータが Notification Parameters タブに表示されます。

**ステップ 3**　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

## サブスクライバ通知の追加

最大 29 のサブスクライバ通知をサービス コンフィギュレーションに追加できます。

**（注）**　サブスクライバ通知を作成しても、サブスクライバ通知機能は有効になりません。サブスクライバ通知を定義したら、特定のパッケージに対してアクティブにする必要があります（「規則のための違反処理パラメータの編集」[p.9-56] を参照）。

**ステップ 1**　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

**ステップ 2**　（**Add**）をクリックします。

**ステップ 3**　新しいサブスクライバ通知の一意の名前を Name フィールドに入力します。

**（注）**　サブスクライバ通知にデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

**ステップ 4**　Destination URL フィールドに宛先 URL を入力します。

**ステップ 5**　通知パラメータを宛先 URL に付ける場合は、**Append notification parameters to URL** チェック ボックスをオンにします。

**ステップ 6**　**Dismissal Method** オプション ボタンのいずれかを選択します。

- **Subscriber browses to the destination URL**
- **The condition that activated the notification no longer holds**
- **Subscriber browses to the dismissal URL**

**ステップ 7**　ステップ 6 で Subscriber browses to the dismissal URL を選択した場合は、表示されるフィールドに解除 URL ホストサフィックスおよびパスプレフィックスを入力します。

**ステップ 8**　Allowed URL テキスト ボックスに、許可 URL を 1 行に 1 つずつ入力します。

**ステップ 9**　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

## サブスクライバ通知の編集

**ステップ 1**　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

**ステップ 2**　Notifications タブでサブスクライバ通知をクリックします。パラメータが表示されます。

**ステップ 3**　サブスクライバ通知のパラメータを Notification Parameters タブで編集します。

**ステップ 4**　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

## サブスクライバ通知の削除

サブスクライバ通知はいつでも削除できます。

デフォルト通知またはネットワーク攻撃通知を削除することはできません。

**ステップ 1**　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

**ステップ 2**　Notifications タブでサブスクライバ通知をクリックします。

**ステップ 3**　（**Delete**）をクリックします。

**ステップ 4**　**Yes** をクリックします。

**ステップ 5**　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

# システム設定の管理

Console では、以下を制御するさまざまなシステム パラメータを判別できます。

- システムの動作状態
- 非対称ルーティング分類モードのイネーブル化とディセーブル化
- リダイレクションをサポートするプロトコルのリダイレクション URL
- BW 優先順位モード（「BW 管理優先順位モードの設定」[p.9-45] を参照）
- 詳細サービス コンフィギュレーション オプション

## システム モードの設定についての情報



### システムの動作モード

Console では、システムの動作モードを選択できます。この機能では、システムがネットワーク トラフィックを処理する方法を定義します。

（注）　各規則には独自の動作モード（状態）があります。これがシステム モードと異なる場合、2 つのモードのうち「下位」のモードが使用されます。たとえば、規則が有効で、システム モードが Report-only の場合、規則は RDR の生成だけを行います。

3 つの動作モードは次のとおりです。

- Full Functionality — システムはアクティブな規則をネットワーク トラフィックで実施し、レポート機能を実行します（つまり、RDR を生成します）。
- Report Only — システムは RDR の生成のみを行います。ネットワーク トラフィックには、アクティブな規則適用は実行されません。
- Transparent — システムは RDR を生成せず、ネットワーク トラフィックにアクティブ規則を適用しません。

### 非対称ルーティング分類モード

Console から非対称ルーティング分類モードをイネーブルにしたりディセーブルにしたりできます。単一方向のフロー レートが高い環境に SCE プラットフォームが配置されている場合、このモードをイネーブルにすると分類の精度を大幅に向上させることができます。ただし、このモードをイネーブルにした場合には、SCA BB の次の機能が使用できません。

- Flavors
- 外部クォータ プロビジョニング
- サブスクライバ通知
- リダイレクション
- Flow Signaling RDR
- コンテンツ フィルタリング
- VAS トラフィック フォワーディング

- 異常検知（非対称ルーティング分類モードでサービス　コンフィギュレーションを作成した場合、すべての異常ディテクタの不審セッション レートとセッション レートが同じに設定されます（「異常検出設定の表示」[p.10-6] を参照）。これにより異常検知は実質的にディセーブルになります。

非対称ルーティング分類モードがイネーブルの場合、Service Configuration Editor には（Problems View 画面に）サービス コンフィギュレーションとこのモードでサポートされる機能が一致するかどうかが表示されます。

次の機能はサービス コンフィギュレーションの一部ではありませんが、非対称ルーティング分類モードがイネーブルの場合に影響を受けます。

- サブスクライバ アウェア モードはサポートされません。
- 拡張フローオープン モードをイネーブルにする必要があります。

上記の機能の状態がルーティング分類モードの状態と一致するかどうかは表示されません。

### プロトコル分類

非対称ルーティング分類モードがイネーブルになっている場合、プロトコル分類は単一方向の UDP フローを除いて通常の方法で実行されます。単一方向 UDP フローのサーバ側を知ることは不可能なので、SCA BB は先頭パケットの宛先ポートを使用してプロトコルを分類します。完全に一致するものが見つからなければ、送信元ポートを使用してプロトコルの分類を試みます。

### 非対称ルーティング分類モードへの切り替え

対称モードでサービス コンフィギュレーションを作成し、非対称ルーティング分類モードに切り替えると、次の状態になります。

- 分類にフレーバは使用されません。
- 定期的なクォータ管理モードが使用されます。
- 非対称ルーティング分類モードに切り替えてもデータは失われませんが、サポートされない機能をすべてサービス コンフィギュレーションから削除するまでは SCE プラットフォームにサービス コンフィギュレーションを適用できません。

### 非対称ルーティング分類モードからの切り替え

非対称ルーティング分類モードでサービス コンフィギュレーションを作成すると、次の状態になります。

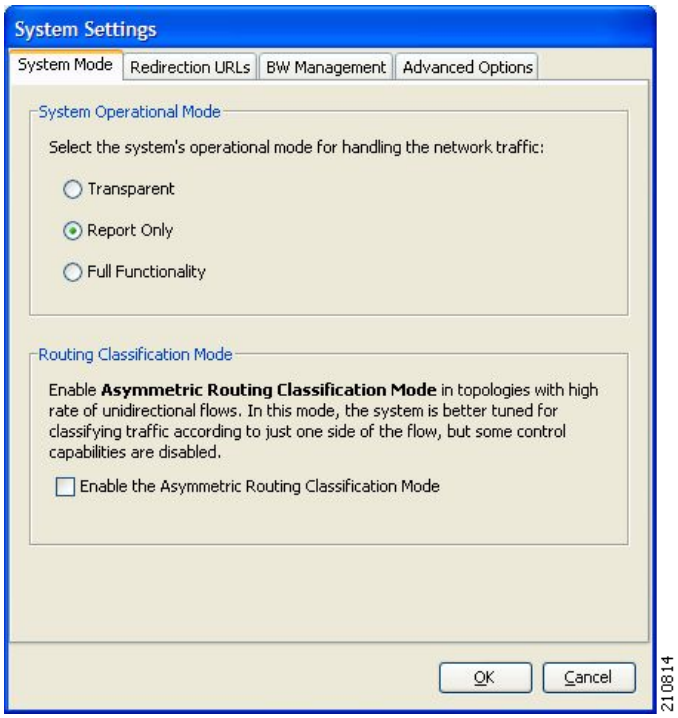
- すべての異常ディテクタの不審セッション レートとセッション レートは同じに設定されます。
- デフォルト サービス コンフィギュレーションにフレーバは作成されず、サービス要素は指定されたフレーバを持ちません。
- クォータ管理モードは、集約時間が 1 日 1 回の定期モードになります。
- 対称モードに切り替えても非対称ルーティング分類モードの制限は保持されます。制限を変更するには、サービス コンフィギュレーションを編集する必要があります。

## システムの動作モードとトポロジ モードの設定

**ステップ 1**　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

**図 10-24**




**ステップ 2**　**System Operational Mode** オプション ボタンのいずれかを選択します。

- **Transparent**
- **Report only**
- **Full functionality**

**ステップ 3**　ルーティング分類モードを変更するには、**Enable the Asymmetric Routing Classification Mode** チェックボックスをオンまたはオフにします。

**ステップ 4**　**OK** をクリックします。

System Settings ダイアログボックスが閉じます。

新しいシステム モード設定が保存されます。

## リダイレクション パラメータの設定

パッケージの規則によって、選択したプロトコルへのアクセスが拒否されることがあります。パッケージのサブスクライバが、ブロックされているプロトコルにアクセスしようとすると（たとえば「ゴールド」サブスクライバのみが使用可能なサービスに「シルバー」サブスクライバがアクセスしようとすると）、トラフィック フローはサーバにリダイレクトされ、リダイレクションの理由についてその Web ページで説明されます。この Web ページにより、パッケージをアップグレードする機会をサブスクライバに提供できます。規則を定義する際に、使用するリダイレクション セットを設定できます（「規則のためのフローごとのアクションの定義」[p.9-15] を参照）。

（注）　リダイレクションは、非対称ルーティング分類モードがイネーブルの場合はサポートされません。

Console のリダイレクション機能では、次の 3 つのプロトコルのみがサポートされます。

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

リダイレクション セットには、これらの 3 つのプロトコルにそれぞれ対応したリダイレクション オプションが 1 つずつ含まれています。システムはデフォルトのリダイレクション セットを提供しますが、これは削除できません。最大で 49 のリダイレクション セットを追加できます。

各リダイレクション URL には、次のフォーマットの URL 指定名、サブスクライバ ID、およびサービス ID が含まれています。

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

## リダイレクション URL セットの追加

最大で 49 のリダイレクション セットを追加できます。

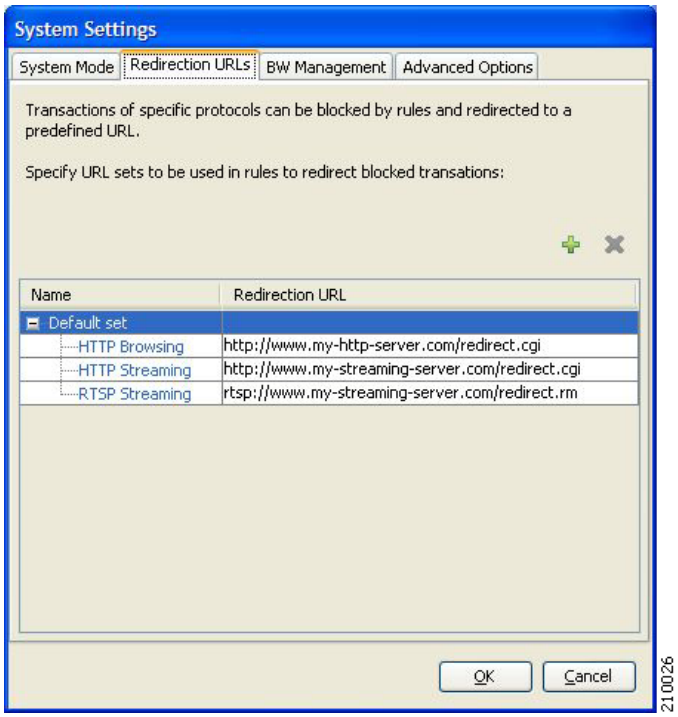
**ステップ 1**　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

**ステップ 2**　**Redirection URLs** タブをクリックします。

Redirection URL タブが開きます。

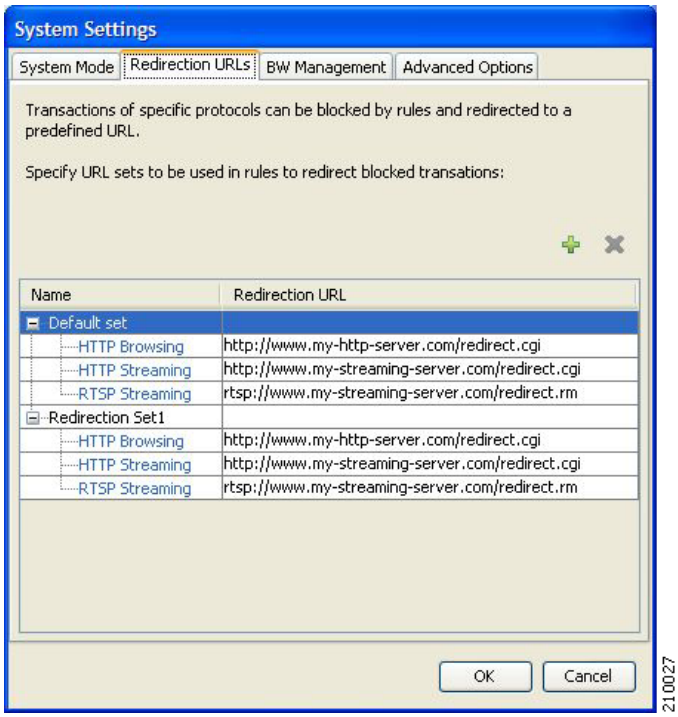
**図 10-25**



**ステップ 3**　（**Add**）をクリックします。

デフォルトのリダイレクション URL を含む新しいリダイレクション セットが、リダイレクション セット リストに追加されます。

**図 10-26**




**ステップ 4**　新しいリダイレクション セットの一意の名前を Name フィールドに入力します。

**（注）**　リダイレクション　セットにデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

**ステップ 5**　新しいリダイレクション セットの Redirection URL セルに新しい値を入力します。

**ステップ 6**　**OK** をクリックします。

System Settings ダイアログボックスが閉じます。

リダイレクション グループがリダイレクション セット リストに追加されます。

## リダイレクション パラメータの編集

**ステップ 1**　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

**ステップ 2**　**Redirection URLs** タブをクリックします。

Redirection URL タブが開きます。

**ステップ 3**　**Redirection URL** カラムの URL をクリックします。

**ステップ 4**　新しい URL を入力します。

**ステップ 5**　**OK** をクリックします。

System Settings ダイアログボックスが閉じます。

リダイレクション設定が保存されます。

## リダイレクション URL セットの削除

**ステップ 1**　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

**ステップ 2**　**Redirection URLs** タブをクリックします。

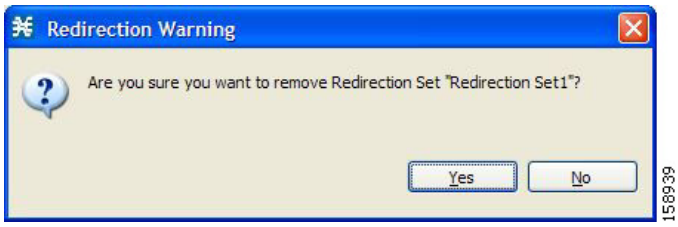
Redirection URL タブが開きます。

**ステップ 3**　リダイレクション セットの名前をクリックします。

**ステップ 4**　（**Delete**）をクリックします。

Redirection Warning メッセージが表示されます。

**図 10-27**



**ステップ 5**　**Yes** をクリックします。

リダイレクション セットが削除されます。

**ステップ 6**　**OK** をクリックします。

System Settings ダイアログボックスが閉じます。

リダイレクション設定が保存されます。

## 詳細サービス コンフィギュレーション オプションの管理

詳細サービス コンフィギュレーション オプションでは、高度であまり変更しないシステム属性を制御します。このオプションは変更しないことを推奨します。

このオプションについて、次の表で説明します。

**表 10-2　詳細サービス コンフィギュレーション プロパティ**

| プロパティ | デフォルト値 | 説明 |
|---|---|---|
| **Classification** | | |
| Classification based on recent classification history enabled | TRUE | 最新分類履歴は学習メカニズムであり、以前のトラフィック分類決定に従ってフローを分類するために使用します。<br>このメカニズムでは、Warez、Skype、Winny2 のフローの分類が改善されます。 |
| Guruguru detailed inspection mode enabled | FALSE | Guruguru プロトコルは、日本で普及している Guruguru ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。<br>• Default — Guruguru トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。<br>• Detailed — Guruguru トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークのみで一般的です。 |
| Kuro detailed inspection mode enabled | FALSE | Kuro プロトコルは、日本で普及している Kuro ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。<br>• Default — Kuro トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。<br>• Detailed — Kuro トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークのみで一般的です。 |

表 10-2　詳細サービス コンフィギュレーション プロパティ（続き）

| プロパティ | デフォルト値 | 説明 |
|---|---|---|
| Soribada detailed inspection mode enabled | FALSE | Soribada プロトコルは、日本で普及している Soribada ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。<br>• Default ― Soribada トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。<br>• Detailed ― Soribada トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークのみで一般的です。 |
| TCP destination port signatures | 1720:H323 | 正しい分類にポート ヒントが必要であるシグニチャの TCP 宛先ポート番号。<br>有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。<br>適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、DHCP です。 |
| UDP destination port signatures | 67:DHCP、<br>1812:Radius Access、<br>1645:Radius Access、<br>1813:Radius Accounting、<br>1646:Radius Accounting | 正しい分類にポート ヒントが必要であるシグニチャの UDP 宛先ポート番号。<br>有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。<br>適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、DHCP です。 |
| UDP ports for which flow should be opened on first packet | 5060, 5061, 67, 69, 1812, 1813, 1645, 1646, 2427, 2727, 9201, 9200, 123, 1900, 5190, 10000 | 拡張フローオープン モードは指定 UDP ポートで無効になり、フローの先頭パケットに従った分類が可能になります。 |
| UDP source port signatures | 1812:Radius Access、<br>1645:Radius Access、<br>1813:Radius Accounting、<br>1646:Radius Accounting | 正しい分類にポート ヒントが必要であるシグニチャの UDP 送信元ポート番号。<br>有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。<br>適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、DHCP です。 |

表 10-2　詳細サービス コンフィギュレーション プロパティ（続き）

| プロパティ | デフォルト値 | 説明 |
|---|---|---|
| V-Share detailed inspection mode enabled | FALSE | V-Share プロトコルは、日本で普及している V-Share ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。<br>• Default — V-Share トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。<br>• Detailed — V-Share トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークのみで一般的です。 |
| Winny detailed inspection mode enabled | FALSE | Winny P2P プロトコルは、日本で普及している Winny ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。<br>• Default — Winny トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。<br>• Detailed — Winny トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークのみで一般的です。 |
| **L7 Filtered Traffic** | | |
| DHT filter enabled | TRUE | DHT フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。 |
| Gnutella 2 Networking filter enabled | TRUE | Gnutella 2 Networking フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。 |
| Gnutella filter enabled | TRUE | Gnutella フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。 |
| L7 filtering enabled | TRUE | L7 Filtered Traffic 機能をイネーブルにするかどうかを指定します。<br>レイヤ 7 フィルタ処理されたフローは SCA プラットフォームに渡されないので、分類、制御、レポートのいずれも行われません。 |
| Warez filter enabled | TRUE | Warez フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。 |

表 10-2　詳細サービス コンフィギュレーション プロパティ（続き）

| プロパティ | デフォルト値 | 説明 |
|---|---|---|
| **Malicious Traffic** | | |
| Malicious Traffic RDRs enabled | TRUE | 悪質トラフィック RDR を生成するかどうかを指定します。 |
| Number of seconds between Malicious Traffic RDRs on the same attack | 60 | 攻撃が検出されると、悪質トラフィック RDR が生成されます。悪質トラフィック RDR は、攻撃が続く間、ユーザが設定した間隔で定期的に生成されます。 |
| TCP port that should remain open for Subscriber Notification | 80 | 検出されたネットワーク攻撃の一部であるフローのブロックを選択できますが、これによって攻撃のサブスクライバ通知が妨害されることがあります。<br>指定 TCP ポートはブロックされず、攻撃通知をサブスクライバに送信できるようになります。 |
| **Policy Check** | | |
| Ongoing policy check mode enabled | TRUE | すでに開いているフローにポリシーの変更が影響するかどうかを指定します。 |
| Time to bypass between policy checks | 30 | すでに開いているフローにポリシーの変更が影響する前に経過する最長時間（秒単位）。 |
| **Quota Management** | | |
| Grace period before first breach | 2 | クォータ制限違反があったあと、違反処理を実行する前に待機する時間（秒単位）。<br>ポリシー サーバではこの時間を使用し、ログインしたサブスクライバにクォータをプロビジョニングします。 |
| Length of the time frame for quota replenish scatter (minutes) | 0 | 定期クォータ補充をランダムに分散する時間帯の長さ。 |
| Time to bypass between policy checks for quota limited flows | 30 | すでに開いているフローにクォータ違反が影響する前に経過する最長時間（秒単位）。 |
| Volume to bypass between policy checks for quota limited flows | 0 | すでに開いているフローにクォータ違反が影響する前に通過する最大フロー ボリューム（バイト単位）。<br>値をゼロにすると、ボリュームが無制限に通過します。 |
| **Reporting** | | |
| Media Flow RDRs enabled | TRUE | メディア フロー RDR を生成するかどうかを指定します。 |
| Subscriber Accounting RDR enabled | FALSE | サブスクライバ課金 RDR を生成するかどうかを指定します。<br>サブスクライバ課金 RDR は、SM-ISG 統合に使用します。詳細については、『*Cisco Service Control Engine (SCE) Software Configuration Guide*』の「Managing the SCMP」の章にある ISG 文書を参照してください。 |

## 詳細サービス コンフィギュレーション オプションの編集

### 手順の詳細

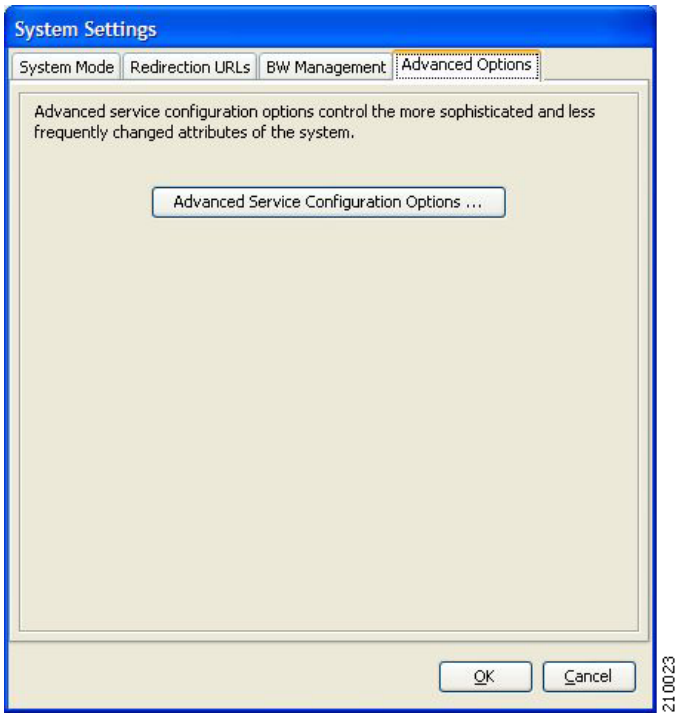
**ステップ 1**　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

**ステップ 2**　**Advanced Options** タブをクリックします。

Advanced Options タブが開きます。

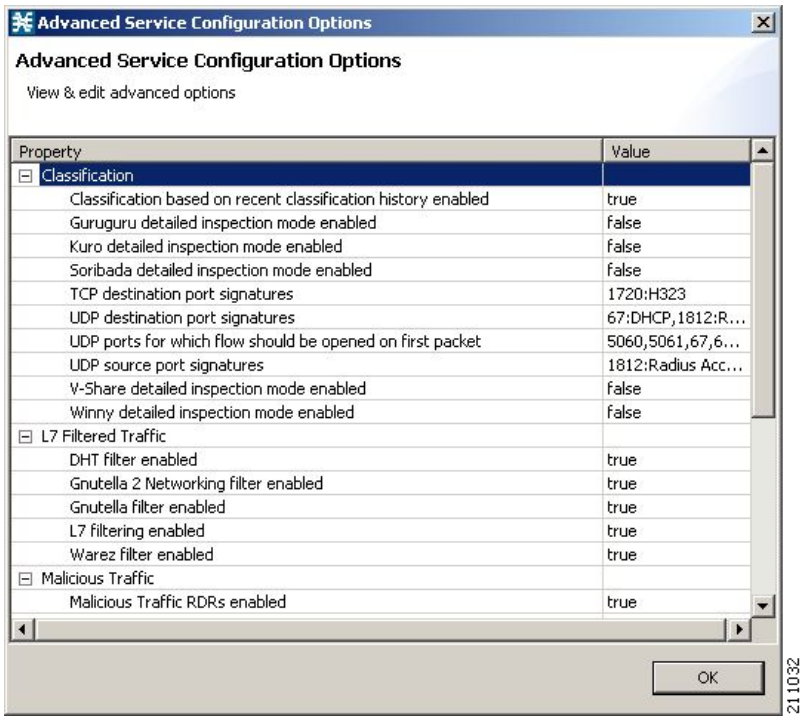
**図 10-28**




**ステップ 3**　**Advanced Service Configuration Options** をクリックします。

Advanced Service Configuration Options ダイアログボックスが開きます。

**図 10-29**




**ステップ 4**　設定オプションを変更します。

**ステップ 5**　**OK** をクリックします。

Advanced Service Configuration Options ダイアログボックスが閉じます。

詳細オプションの変更が保存されます。

## VAS トラフィック フォワーディング設定の管理

Value Added Service（VAS）サーバへのトラフィック フォワーディングでは、侵入検知やサブスクライバのコンテンツ フィルタリングなどの詳細トラフィック処理に外部エキスパート システム（VAS サーバ）を使用できます。フローは処理後に SCE プラットフォームに送り返され、SCE プラットフォームはフローを元の宛先に送信します。

フォワーディングされるフローは、サブスクライバ パッケージおよびフロー タイプ（IP プロトコル タイプおよび宛先ポート番号）に基づいて選択されます。

VAS トラフィック フォワーディングには次の制限があります。

- SCE 2000 4xGBE プラットフォームのみが VAS トラフィック フォワーディングをサポートします。
- 1 つの SCE プラットフォームで 8 までの VAS サーバをサポートできます。
- サービス コンフィギュレーションには、最大 64 のトラフィックフォワーディング テーブルを含めることができます。

- トラフィックフォワーディング テーブルには、64 までのテーブル パラメータを含めることができます。
- VAS トラフィック フォワーディングは、非対称ルーティング分類モードではサポートされません。

（注）　VAS トラフィックフォワーディング機能は複雑なので、VAS フローはグローバル帯域幅制御に影響されません。

VAS トラフィックフォワーディングを使用するには、SCE プラットフォームで VAS サービスを設定する必要もあります。詳細については、『*Cisco Service Control Engine (SCE) Software Configuration Guide*』の「Value Added Services (VAS) Traffic Forwarding」の章を参照してください。

### VAS トラフィック フォワーディングの有効化

デフォルトの場合、VAS トラフィック フォワーディングは無効になっています。VAS トラフィック フォワーディングはいつでも有効にすることができます。

（注）　VAS トラフィック フォワーディングは、非対称ルーティング分類モードではサポートされません。

### VAS トラフィック フォワーディングの有効化

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Enable Traffic Forwarding to VAS Servers** チェック ボックスをオンにします。

（注）　VAS トラフィック フォワーディングは、非対称ルーティング分類モードではサポートされません。非対称ルーティング分類モードがイネーブルのときに Enable Traffic Forwarding to VAS Servers チェックボックスをオンにしようとした場合は、VAS Error メッセージが表示されます。

**OK** をクリックし、ステップ 3 に進みます。

Package Settings ダイアログボックスの Advanced タブの VAS Traffic Forwarding Table ドロップダウン リストが有効になります（「高度なパッケージ オプションの設定」[p.9-7] を参照）。

**ステップ 3**　**Close** をクリックします。

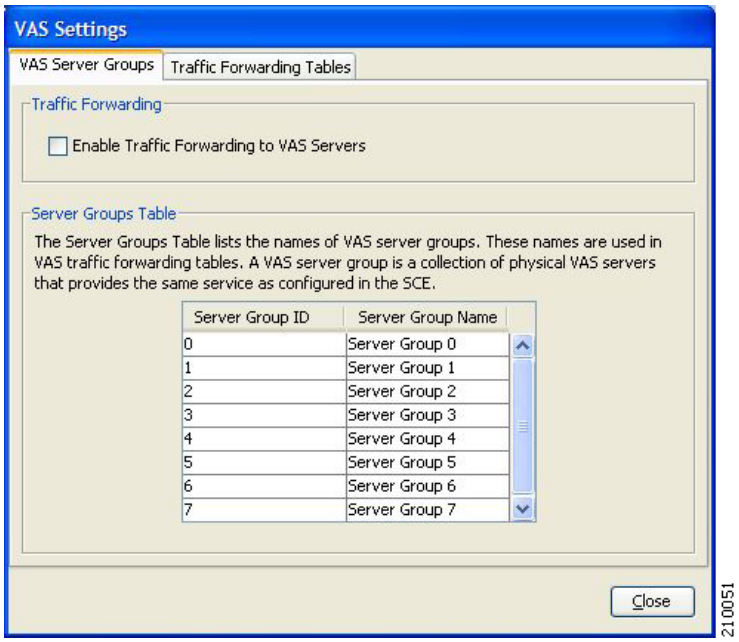
VAS Settings ダイアログボックスが閉じます。

### VAS トラフィック フォワーディングの無効化

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**図 10-30**




**ステップ 2**　**Enable Traffic Forwarding to VAS Servers** チェック ボックスをオフにします。

VAS トラフィック フォワーディングが無効になります。

**ステップ 3**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

## VAS サーバ グループの名前変更

SCE プラットフォームでは、8 までの VAS サーバ グループにフローを転送できます。デフォルトの場合、8 つのサーバ グループには、「Server Group n」（n は 0 ～ 7 の値）という名前が付きます。サーバ グループにわかりやすい名前を付けてください。付けた名前は、Package Settings ダイアログボックスの Advanced タブのドロップダウン リスト（「高度なパッケージ オプションの設定」[p.9-7] を参照）、および各トラフィックフォワーディング テーブルに追加したテーブル パラメータの Server Group フィールド（「VAS テーブル パラメータの管理」[p.10-51] を参照）に表示されます。

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

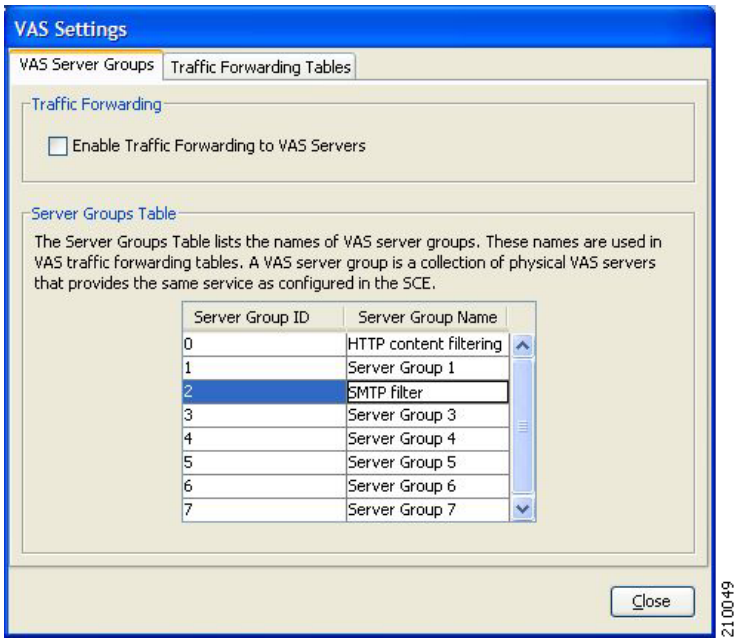
VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　Server Groups Table 領域のテーブルで、サーバ グループ名を含むセルをダブルクリックします。

**ステップ 3**　わかりやすい名前をセルに入力します。

**ステップ 4**　名前を変更するその他のサーバ グループに、ステップ 2 および 3 を繰り返します。

**図 10-31**




**ステップ 5**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

## VAS トラフィック フォワーディング テーブルの表示

SCA BB は、SCE プラットフォームを通過するフローを VAS サーバ グループに転送するかどうかをトラフィックフォワーディング テーブルに基づいて判断します。トラフィックフォワーディング テーブルの各エントリ（テーブル パラメータ）では、特定フローをどの VAS サーバ グループに転送するかが定義されます。

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

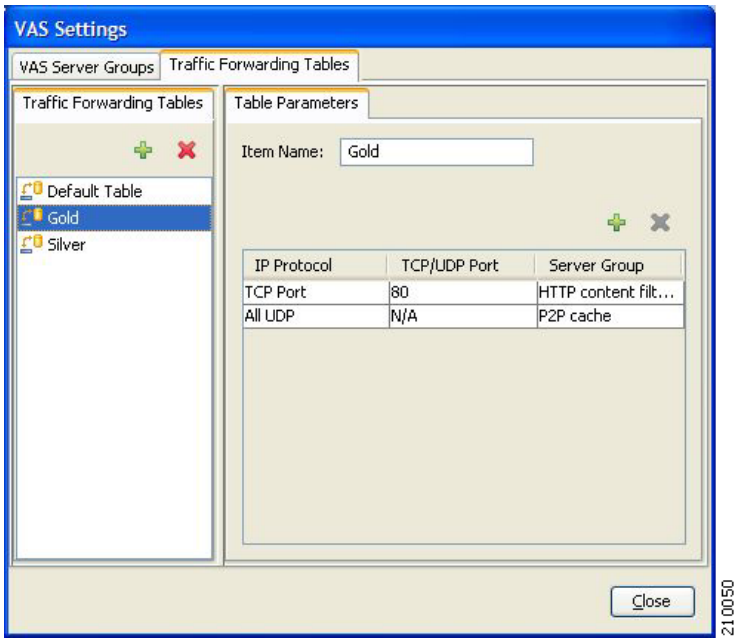
Traffic Forwarding Tables タブが開きます。

すべてのトラフィックフォワーディング テーブルのリストが、Traffic Forwarding Tables 領域に表示されます。

**ステップ 3**　トラフィックフォワーディング テーブルのリストのテーブルをクリックし、テーブル パラメータを表示します。

トラフィックフォワーディング テーブルに定義されているすべてのテーブル パラメータのリストが、Table Parameters タブに表示されます。

**図 10-32**




**ステップ 4**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

## VAS トラフィック フォワーディング テーブルの削除

ユーザが作成したすべてのトラフィックフォワーディング テーブルを削除できます。デフォルト トラフィックフォワーディング テーブルを削除することはできません。

（注）　パッケージに関連しているトラフィックフォワーディング テーブルを削除することはできません。

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

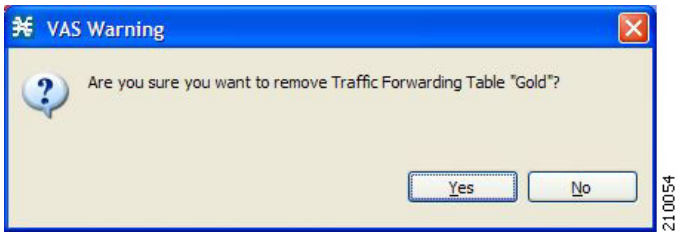
Traffic Forwarding Tables タブが開きます。

**ステップ 3**　Traffic Forwarding Tables 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

**ステップ 4**　（**Delete**）をクリックします。

VAS Warning メッセージが表示されます。

**図 10-33**




**ステップ 5**　**Yes** をクリックします。

選択したテーブルが削除され、トラフィックフォワーディング テーブルのリストに表示されなくなります。

**ステップ 6**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

## VAS トラフィック フォワーディング テーブルの追加

サービス コンフィギュレーションにはデフォルト トラフィックフォワーディング テーブルが組み込まれています。最大 63 のトラフィックフォワーディング テーブルをさらに追加し、さまざまなトラフィックフォワーディング テーブルを別々のパッケージに割り当てることができます。

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

Traffic Forwarding Tables タブが開きます。

**ステップ 3**　Traffic Forwarding Tables 領域で　（**Add**）をクリックします。

「Table (n)」（n は 1 ～ 63 の値）という名前の新しいテーブルが、Traffic Forwarding Tables 領域のトラフィックフォワーディング テーブルのリストに追加されます。

テーブル名は、Table Parameters タブの Item Name ボックスにも表示されます。

**ステップ 4**　トラフィックフォワーディング テーブルの一意でわかりやすい名前を Item Name フィールドに入力します。

新しいトラフィックフォワーディング テーブルにはテーブル パラメータを追加できます（「VAS テーブル パラメータの追加」[p.10-51] を参照）。

## VAS テーブル パラメータの管理

テーブル パラメータは、IP プロトコル タイプ、関連 TCP/UDP ポート（該当する場合）、VAS サーバ グループまたは IP アドレスの範囲です。

トラフィックフォワーディング テーブルは関連テーブル パラメータの集合です。

トラフィックフォワーディング テーブルには、64 までのテーブル パラメータを含めることができます。

### VAS テーブル パラメータの追加

最大 64 のテーブル パラメータをトラフィックフォワーディング テーブルに追加できます。

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

Traffic Forwarding Tables タブが開きます。

**ステップ 3**　Traffic Forwarding Tables 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

**ステップ 4**　Traffic Parameters タブで、（**Add**）をクリックします。

Table Parameters タブのテーブル パラメータのリストに、新しいテーブル パラメータが追加されます。

**（注）**　それぞれの新しいテーブル パラメータには、次のデフォルト値が含まれます。

| |
|---|
| IP プロトコル = TCP ポート |
| TCP/UDP ポート = 80 |
| サーバ グループ = Server Group 0 |

次のセクションで説明するように、新しいテーブル パラメータをここで編集できます。

**ステップ 5**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

### VAS テーブル パラメータの編集

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

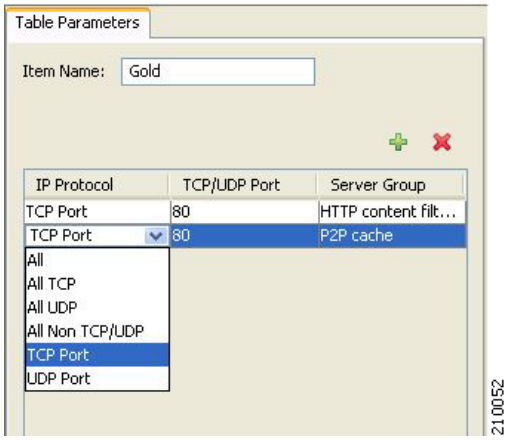
Traffic Forwarding Tables タブが開きます。

**ステップ 3**　Traffic Forwarding Tables 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

**ステップ 4**　Table Parameters タブのテーブルで次のように操作します。

1. IP Protocol カラムのセルをクリックし、表示されるドロップダウン リストから IP プロトコル タイプを選択します。

**図 10-34**

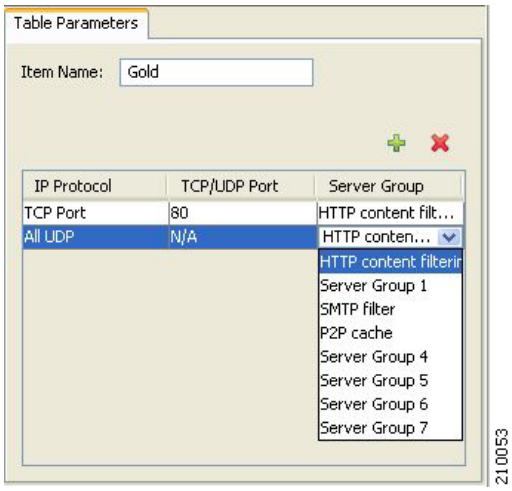



2. All、All TCP、All UDP、All Non TCP/UDP のうちいずれかを選択した場合は、テーブルの別のセルに移動したとき、TCP/UDP Port セルに「N/A」と表示されます。
3. TCP Port または UDP Port を選択した場合は、TCP/UDP Port カラムのセルをダブルクリックし、ポート番号を入力します。

（注）　ポートの範囲を TCP/UDP Port セルに入力することはできません。ポートごとに別のテーブル パラメータを追加する必要があります。

4. Server Group カラムのセルをクリックし、表示されるドロップダウン リストからサーバ グループを選択します。

**図 10-35**




**ステップ 5**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

---

### VAS テーブル パラメータの削除

---

**ステップ 1**　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

VAS Settings ダイアログボックスが表示されます。

**ステップ 2**　**Traffic Forwarding Tables** タブをクリックします。

Traffic Forwarding Tables タブが開きます。

**ステップ 3**　Traffic Forwarding Tables 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

**ステップ 4**　Table Parameters タブのテーブル パラメータのリストからテーブル パラメータを選択します。

**ステップ 5**　（**Delete**）をクリックします。

選択したテーブル パラメータが削除され、テーブル パラメータのリストに表示されなくなります。

**ステップ 6**　**Close** をクリックします。

VAS Settings ダイアログボックスが閉じます。

---