CHAPTER 16

# ASA および Cisco クラウド Web セキュリティ

Cisco クラウド Web セキュリティ では、Software as a Service（SaaS）による Web セキュリティおよび Web フィルタリング サービスが提供されます。ネットワークでASAを使用している企業は、追加ハードウェアをインストールせずに クラウド Web セキュリティ サービスを使用できます。

ASA でクラウド Web セキュリティがイネーブルになっている場合、ASA は、選択された HTTP および HTTPS トラフィックを クラウド Web セキュリティ プロキシ サーバに透過的にリダイレクトします。クラウド Web セキュリティ プロキシ サーバは、コンテンツをスキャンし、Cisco ScanCenter で設定されたポリシーに基づいてトラフィックに関する警告を許可、ブロック、または送信して、許容範囲での使用を促進し、マルウェアからユーザを保護します。

ASA は、任意でアイデンティティ ファイアウォール（IDFW）および AAA ルールによりユーザを認証および識別できます。ASA は、ユーザ クレデンシャル（ユーザ名またはユーザ グループ、あるいはその両方を含む）を暗号化して、クラウド Web セキュリティにリダイレクトするトラフィックに含めます。クラウド Web セキュリティ サービスは、このユーザ クレデンシャルを使用して、ポリシーとトラフィックを照合します。また、ユーザベースのレポーティングでもこのクレデンシャルを使用します。ASA は、ユーザ認証を行わずに（オプションの）デフォルトのユーザ名またはグループ、あるいはその両方を指定できます。ただし、クラウド Web セキュリティ サービスがポリシーを適用するために、ユーザ名とグループは必要ありません。

サービス ポリシー ルールを作成するときに、クラウド Web セキュリティに送信するトラフィックをカスタマイズできます。また、サービス ポリシー ルールに一致する Web トラフィックのサブセットが最初に要求された Web サーバに代わりに直接移動し、クラウド Web セキュリティ にスキャンされないように、「ホワイトリスト」を設定できます。

プライマリおよびバックアップ クラウド Web セキュリティ プロキシ サーバを設定できます。ASA は各サーバを定期的にポーリングして、可用性を確認します。

**（注）** この機能は「ScanSafe」とも呼ばれるため、一部のコマンドには ScanSafe 名が表示されます。

# Cisco クラウド Web セキュリティについて



## クラウド Web セキュリティへの Web トラフィックのリダイレクト

エンド ユーザが HTTP または HTTPS 要求を送信すると、ASA はその要求を受信し、オプションでユーザやグループの情報を取得します。トラフィックがクラウド Web セキュリティの ASA サービス ポリシー ルールと一致した場合、ASA は要求をクラウド Web セキュリティ プロキシ サーバにリダイレクトします。ASA は、プロキシ サーバへの接続のリダイレクトによって、エンド ユーザとクラウド Web セキュリティ プロキシ サーバの間の仲介役として機能します。ASA は、クライアント要求の宛先 IP アドレスおよびポートを変更し、クラウド Web セキュリティに固有の HTTP ヘッダーを追加して、クラウド Web セキュリティ プロキシ サーバに変更された要求を送信します。クラウド Web セキュリティ HTTP ヘッダーには、ユーザ名、ユーザ グループなど、さまざまな種類の情報が含まれています（使用可能な場合）。

## ユーザ認証およびクラウド Web セキュリティ

ユーザ アイデンティティは、クラウド Web セキュリティでポリシーを適用するために使用できます。また、ユーザ アイデンティティは、クラウド Web セキュリティ レポーティングにも役立ちます。クラウド Web セキュリティを使用するには、ユーザ アイデンティティは必要はありません。クラウド Web セキュリティ ポリシーのトラフィックを識別する他の方法があります。

ASA は、ユーザのアイデンティティを決定したり、デフォルト アイデンティティを提供したりする次の方式をサポートします。

- AAA ルール：ASA が AAA ルールを使用してユーザ認証を実行すると、ユーザ名が AAA サーバまたはローカル データベースから取得されます。AAA ルールによるアイデンティティには、グループ情報が含まれていません。設定されている場合は、デフォルトのグループが使用されます。AAA ルールの設定については、従来の機能ガイドを参照してください。
- IDFW：ASA が Active Directory（AD）で IDFW を使用すると、アクセス ルールなどの機能またはサービス ポリシーで ACL を使用するか、ユーザ アイデンティティ モニタを設定してユーザ アイデンティティ情報を直接ダウンロードして、ユーザやグループをアクティブ化したときに、AD エージェントからユーザ名およびグループが取得されます。

  IDFW の設定方法については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。
- デフォルトのユーザ名とグループ：ASA は、ユーザ認証を使用せずに、クラウド Web セキュリティ サービス ポリシー ルールと一致するすべてのユーザのオプションのデフォルトのユーザ名やグループを使用します。

# 認証キー

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。認証キーを使用して、クラウド Web セキュリティは、Web 要求に関連付けられた会社を識別し、ASA が有効なカスタマーに関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれか 1 つを使用できます。

- 「企業認証キー」（P.16-3）
- 「グループ認証キー」（P.16-3）

## 企業認証キー

企業認証キーは、企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスをイネーブルにします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

## グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスをイネーブルにします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

ポリシーにグループ認証キーを使用する方法については、「ScanCenter ポリシー」（P.16-4）を参照してください。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

# ScanCenter ポリシー

ScanCenter では、トラフィックは、ルールに一致するまで順にルールに照合されます。その後、クラウド Web セキュリティがルールの設定済みのアクションを適用します。ユーザ トラフィックはグループの関連付け（*ディレクトリ グループ*または*カスタム グループ*）に基づいて ScanCenter ポリシー ルールと照合できます。


- 「ディレクトリ グループ」（P.16-4）
- 「カスタム グループ」（P.16-4）
- 「グループおよび認証キーの相互運用の仕組み」（P.16-5）


## ディレクトリ グループ

ディレクトリ グループはトラフィックが属するグループを定義します。グループが存在する場合、グループは、クライアント要求の HTTP ヘッダーに含まれています。ASA は、IDFW を設定すると HTTP ヘッダーにグループを含めます。IDFW を使用しない場合は、クラウド Web セキュリティ インスペクションの ASA ルールに一致するトラフィックのデフォルト グループを設定できます。

ディレクトリ グループを設定する場合、グループ名を正確に入力する必要があります。

- IDFW グループ名は次の形式で送信されます。

  *domain-name\group-name*

  ASA が IDFW グループ名を学習すると、ASA での形式は *domain-name\\group-name* となります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。

- デフォルト グループ名は次の形式で送信されます。

  [*domain*\]*group-name*

  ASA では、オプションのドメイン名を 2 つのバックスラッシュ（\\）が続くように設定する必要があります。ただし、一般的な ScanCenter 表記に準拠させるため、ASA はバックスラッシュ（\）を 1 つだけ使用するように名前を変更します。たとえば、「Cisco\\Boulder1」と指定すると、ASA は、グループ名をクラウド Web セキュリティに送信するときに、バックスラッシュ（\）を 1 つのみ使用する「Cisco\Boulder1」に変更します。

## カスタム グループ

カスタム グループは、次の 1 つ以上の基準を使用して定義されます。

- ScanCenter グループ認証キー：カスタム グループのグループ認証キーを生成できます。その後、ASA を設定するときにこのグループ キーを識別すると、ASA からのすべてのトラフィックがグループ キーでタグ付けされます。

- 送信元 IP アドレス：カスタム グループの送信元 IP アドレスを特定できます。ASA サービス ポリシーが送信元 IP アドレスに基づくため、代わりに ASA で IP アドレスベースのポリシーを設定することもできます。
- ユーザ名：カスタム グループのユーザ名を識別できます。
  - IDFW ユーザ名は次の形式で送信されます。

    *domain-name**username*
  - RADIUS または TACACS+ を使用する場合、AAA ユーザ名は次の形式で送信されます。

    LOCAL*username*
  - LDAP を使用する場合、AAA ユーザ名は次の形式で送信されます。

    *domain-name**username*
  - デフォルトのユーザ名は、次の形式で送信されます。

    [*domain-name*\]*username*

    たとえば「ゲスト」としてデフォルトのユーザ名を設定する場合、ASA は「ゲスト」を送信します。「Cisco \ゲスト」としてデフォルトのユーザ名を設定する場合は、ASA は「Cisco \ゲスト」を送信します。

## グループおよび認証キーの相互運用の仕組み

カスタム group+group キーが提供する ASA ごとのポリシーが必要ない場合は、企業キーを使用します。すべてのカスタム グループがグループ キーに関連付けられているわけではありません。キーを使用しないカスタム グループを使用して、IP アドレスまたはユーザ名を識別できます。また、キーを使用しないカスタム グループは、ディレクトリ グループを使用するルールとともにポリシー内で使用できます。

ASA ごとのポリシーが必要であり、グループ キーを使用している場合でも、ディレクトリ グループおよびキーを使用しないカスタム グループによって提供される照合機能を使用できます。この場合、グループ メンバーシップ、IP アドレス、またはユーザ名に基づいていくつかの例外を除いて ASA ベースのポリシーが必要になる場合があります。たとえば、すべての ASA 間で America\Management グループのユーザを除外する場合は、次の手順を実行します。

1. America\Management 用のディレクトリ グループを追加します。
2. このグループに対する免除ルールを追加します。
3. 免除ルールの後に各カスタム group+group キーのルールを追加して、ASA ごとのポリシーを適用します。
4. America\Management のユーザからのトラフィックは免除ルールに一致し、その他すべてのトラフィックは発信元の ASA のルールに一致します。

キー、グループ、およびポリシー ルールの組み合わせが可能です。

# クラウド Web セキュリティのアクション

設定されたポリシーの適用後、クラウド Web セキュリティは、ユーザ要求をブロック、許可、またはユーザ要求に関する警告を送信します。

- 許可：クラウド Web セキュリティは、クライアント要求を許可する場合、最初の要求先サーバにアクセスし、データを取得します。サーバ応答が ASA に転送され、ここからユーザに転送されます。

- ブロック：クラウド Web セキュリティは、クライアント要求をブロックする場合、アクセスがブロックされたことをユーザに通知します。HTTP 302「Moved Temporarily」応答が、クライアント アプリケーションを クラウド Web セキュリティ プロキシ サーバでホストされている Web ページに送信され、ブロック エラー メッセージが表示されます。ASA はクライアントに 302 応答を転送します。
- 警告：サイトにアクセプタブル ユース ポリシー違反があることをクラウド Web セキュリティ プロキシ サーバが決定すると、サイトに関する警告ページが表示されます。警告を挿入し、接続要求をドロップすることも、警告をクリックし、要求されたサイトに進むこともできます。

ASA がプライマリまたはバックアップ クラウド Web セキュリティ プロキシ サーバに到達できない場合の、ASA による Web トラフィックの処理方法を選択できます。これにより、すべての Web トラフィックがブロックされたり、許可されたりする可能性があります。デフォルトでは、Web トラフィックをブロックします。

# ホワイトリストを使用したスキャンのバイパス

AAA ルールまたは IDFW を使用する場合、その他の場合にはサービス ポリシー ルールに一致する特定のユーザまたはグループからの Web トラフィックがスキャンのためクラウド Web セキュリティ プロキシ サーバにリダイレクトされないように ASA を設定できます。クラウド Web セキュリティ スキャンをバイパスすると、ASA はプロキシ サーバに接続せず、最初に要求された Web サーバからコンテンツを直接取得します。Web サーバから応答を受け取ると、データをクライアントに送信します。このプロセスはトラフィックの「ホワイトリスト」といいます。

ACL を使用してクラウド Web セキュリティに送信するトラフィックのクラスを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

# IPv4 および IPv6 のサポート

クラウド Web セキュリティは、現在 IPv4 アドレスだけをサポートしています。IPv6 を内部的に使用する場合は、クラウド Web セキュリティに送信する必要がある IPv6 フローに対して NAT 64 を実行する必要があります。

次の表に、クラウド Web セキュリティ リダイレクションでサポートされるクラス マップ トラフィックを示します。

| クラス マップ トラフィック | クラウド Web セキュリティ インスペクション |
|---|---|
| IPv4 から IPv4 | サポートあり |
| IPv6 から IPv4（NAT64 を使用） | サポートあり |
| IPv4 から IPv6 | 未サポート |
| IPv6 から IPv6 | 未サポート |

## プライマリ プロキシ サーバからバックアップ プロキシ サーバへのフェールオーバー

Cisco クラウド Web セキュリティ サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。

クライアントがプライマリ サーバに到達できない場合、ASA は可用性を判定するためにタワーのポーリングを開始します。（クライアントのアクティビティが存在しない場合、ASA は 15 秒ごとにポーリングします）。設定された回数だけ再試行してもプロキシ サーバが使用できない場合（デフォルトは 5 回。この設定は設定可能）、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

クライアントまたは ASA が、再試行回数に到達する前に少なくとも 2 回連続してサーバに到達できる場合、ポーリングは停止し、タワーはアクセス可能であると判定されます。

バックアップ サーバへのフェールオーバー後、ASA はプライマリ サーバをポーリングし続けます。プライマリ サーバが到達可能になると、ASA はプライマリ サーバの使用に戻ります。

# Cisco クラウド Web セキュリティのライセンス要件

| モデル | ライセンス要件 |
|---|---|
| ASAv | 標準または Premium ライセンス |
| 他のすべてのモデル | ASA とクラウド Web セキュリティ サーバ間のトラフィックを暗号化する高度暗号化（3DES/AES）ライセンス。 |

クラウド Web セキュリティ側では、Cisco クラウド Web セキュリティ ライセンスを購入し、ASA が処理するユーザの数を特定する必要があります。その後、ScanCenter にログインし、認証キーを生成します。

# クラウド Web セキュリティの前提条件

**（オプション）ユーザ認証の前提条件**

クラウド Web セキュリティにユーザ アイデンティティ情報を送信するには、ASA で次のいずれかを設定します。

- AAA ルール（ユーザ名のみ）：従来の機能ガイドを参照してください。
- IDFW （ユーザ名およびグループ）：『一般的な操作のコンフィギュレーション ガイド』を参照してください。

**（オプション）完全修飾ドメイン名の前提条件**

サービス ポリシー ルールまたはクラウド Web セキュリティ サーバに対して ACL で FQDN を使用する場合は、『一般的な操作のコンフィギュレーション ガイド』に従って ASA の DNS サーバを設定する必要があります。

# ガイドラインと制限事項

### コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

マルチ コンテキスト モードでは、サーバ設定はシステム内だけで使用でき、サービス ポリシー ルールの設定はセキュリティ コンテキスト内だけで使用できます。

各コンテキストには、必要に応じて独自の認証キーを設定できます。

### ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

### IPv6 のガイドライン

IPv6 はサポートされません。「IPv4 および IPv6 のサポート」（P.16-6）を参照してください。

### その他のガイドライン

- クラウド Web セキュリティは、ASA クラスタリングではサポートされません。
- クライアントレス SSL VPN はクラウド Web セキュリティではサポートされません。クラウド Web セキュリティの ASA サービス ポリシーからクライアントレス SSL VPN トラフィックを免除してください。
- クラウド Web セキュリティ プロキシ サーバへのインターフェイスがダウンすると、**show scansafe server** コマンドは、約 15 ～ 25 分間、両方のサーバを示します。この状態が発生する原因は、ポーリング メカニズムがアクティブな接続に基づいていること、また、そのインターフェイスがダウンしており、ゼロ接続を示し、ポーリング時間が最も長い方法が使用されることなどです。
- クラウド Web セキュリティは、ASA CX モジュールではサポートされません。同じトラフィックに対して ASA CX アクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA CX アクションのみを実行します。
- クラウド Web セキュリティ インスペクションは同じトラフィックの HTTP インスペクションと互換性があります。HTTP インスペクションは、デフォルト グローバル ポリシーの一部としてデフォルトでイネーブルになっています。
- クラウド Web セキュリティは、別の接続に対して同じ送信元ポートおよび IP アドレスを使用できる可能性がある拡張 PAT またはアプリケーションではサポートされません。たとえば、2 つの異なる接続（別個のサーバへの接続）が拡張 PAT を使用する場合、これらの接続は別個の宛先によって区別されているため、ASA は、両方の接続変換に同じ送信元 IP および送信元ポートを再利用する可能性があります。ASA がこれらの接続をクラウド Web セキュリティ サーバにリダイレクトすると、宛先がクラウド Web セキュリティ サーバの IP アドレスおよびポート（デフォルトは 8080）に置き換えられます。その結果、接続は両方とも、同じフロー（同じ送信元 IP/ポートおよび宛先 IP/ポート）に属しているように見え、リターン トラフィックが適切に変換解除されません。
- この Default Inspection Traffic トラフィック クラスには、クラウド Web セキュリティ インスペクションのデフォルト ポートは含まれません（80 および 443）。

# デフォルト設定

デフォルトでは、Cisco クラウド Web セキュリティはイネーブルになりません。

# Cisco クラウド Web セキュリティ の設定



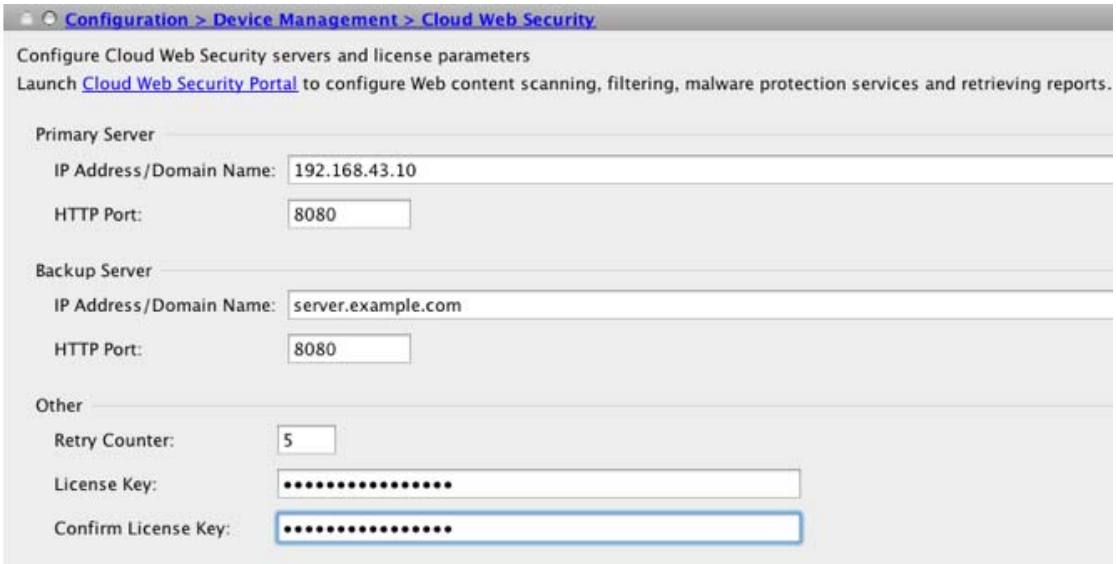
## クラウド Web セキュリティ プロキシ サーバとの通信の設定

### ガイドライン

公開キーは ASA ソフトウェアに組み込まれているため、設定する必要がありません。

### 手順の詳細

**ステップ 1**　[Configuration] > [Device Management] > [Cloud Web Security] を選択します。




**ステップ 2**　[Primary Server] 領域で、次の情報を入力します。

- [IP Address/Domain Name]：プライマリ サーバの IPv4 アドレスまたは FQDN を入力します。

- [HTTP Port]：プライマリ サーバの HTTP ポート（トラフィックをリダイレクトする必要があるポート）を入力します。デフォルトでは、ポートは 8080 です。リダイレクトするポートを変更しない限り、この値を変更しないでください。

**ステップ 3**　[Backup Server] 領域で、次の情報を入力します。

- [IP Address/Domain Name] : バックアップ サーバの IPv4 アドレスまたは FQDN を入力します。
- [HTTP Port]：バックアップ サーバの HTTP ポート（トラフィックをリダイレクトする必要があるポート）を入力します。デフォルトでは、ポートは 8080 です。有効な値は 1 ～ 65535 です。

**ステップ 4**　[Other] 領域で、次の情報を入力します。

- [Retry Counter]：サーバが到達不能であると判定する前に、クラウド Web セキュリティ プロキシ サーバに対するポーリングに連続して失敗した回数を示す値を入力します。ポーリングは、30 秒ごとに実行されます。有効な値は 2 ～ 100 で、デフォルトは 5 です。
- [License Key]：要求の送信元の組織を示すために、ASA が クラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。認証キーは 16 バイトの 16 進数です。「認証キー」（P.16-3）を参照してください。
- [Confirm License Key]：認証キーを確認します。

**ステップ 5**　[Apply] をクリックします。

# （マルチ コンテキスト モード）セキュリティ コンテキストごとのクラウド Web セキュリティの許可

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

（注）　管理コンテキストおよび特定のコンテキスト両方の Scansafe タワーに対応するルートを設定する必要があります。これは Scansafe タワーがアクティブ/アクティブ フェールオーバーのシナリオで到達不能にならないことを保障します。

# クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法

サービス ポリシーは、複数のサービス ポリシー ルールで構成され、グローバルに適用されるか、またはインターフェイスごとに適用されます。各サービス ポリシー ルールでは、クラウド Web セキュリティへのトラフィックを送信するか（Match）、またはクラウド Web セキュリティからのトラフィックを除外するか（Do Not Match）のいずれかを指定できます。インターネット宛に送信されるトラフィックのルールを作成します。これらのルールの順序は重要です。ASA がパケットを転送するか除外するかを判断する場合、ASA は、ルールがリストされている順序で、各ルールによってパケットをテストします。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、すべてのトラフィックが明示的に一

致するルールをポリシーの冒頭に作成した場合、残りのステートメントは一切チェックされません。ポリシーの追加後、必要に応じてルールの順序を変更できます。

サービス ポリシー ルールの詳細については、第 1 章「サービス ポリシー」を参照してください。

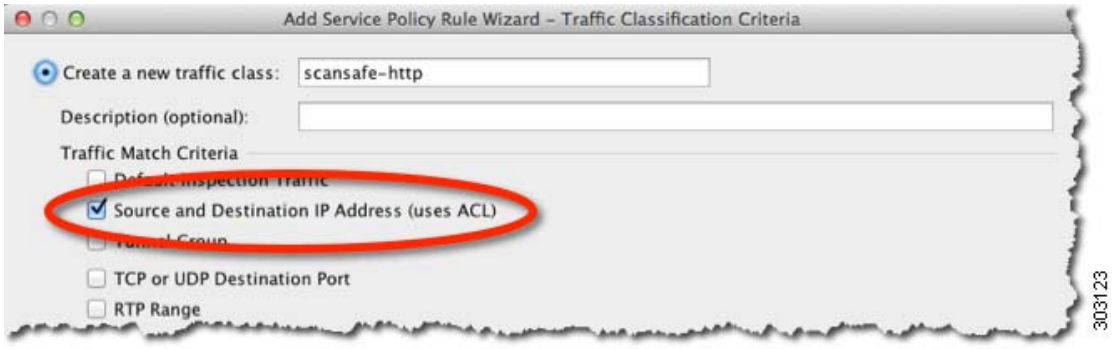
## 前提条件

（オプション）ホワイトリストを使用して一部のトラフィックをクラウド Web セキュリティへの送信から免除する必要がある場合は、サービス ポリシー ルールでホワイトリストを参照できるように、最初に「（オプション）ホワイトリストに記載されたトラフィックの設定 」（P.16-24）に従ってホワイトリストを作成します。

## 手順の詳細

**ステップ 1**　サービス ポリシー ルールを追加するには、[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。

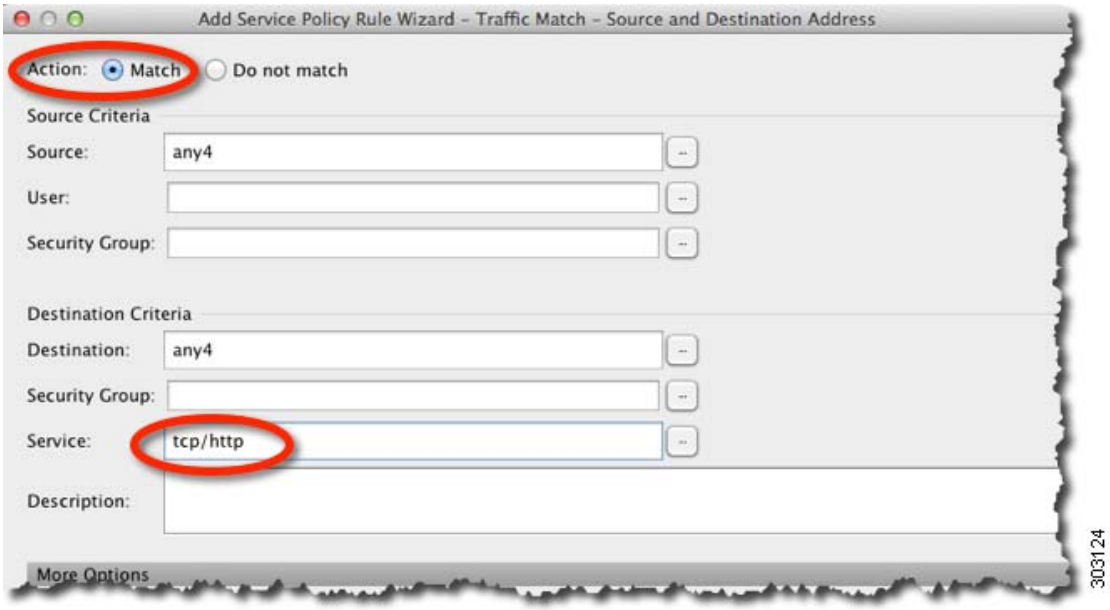
**ステップ 2**　[Service Policy] ダイアログボックスで、新しいサービス ポリシーの一部としてクラウド Web セキュリティを設定するか、または、既存のサービス ポリシーを編集できます。[Next] をクリックします。




**ステップ 3**　[Traffic Classification Criteria] ダイアログボックスで、トラフィック クラスに名前を付け（またはデフォルト名を受け入れて）、[Create a new traffic class] オプションを選択したままにし、[Source and Destination IP address (Uses ACL)] をクリックして、[Next] をクリックします。

このタイプの新しいトラフィック クラスを作成する場合は、最初にアクセス コントロール エントリ（ACE）を 1 つだけ指定できます。ルールを追加した後は、同じインターフェイスまたはグローバル ポリシーに新しいルールを追加し、それから [Traffic Classification] ダイアログボックスで [Add rule to existing traffic class] を指定することによって、ACE を追加できます。

[Traffic Match - Source and Destination] ダイアログボックスが表示されます。




**a.** [Match] または [Do Not Match] をクリックします。

[Match] は送信元および宛先に一致するトラフィックがクラウド Web セキュリティに送信されるように指定します。[Do Not Match] は一致したトラフィックをクラウド Web セキュリティから除外します。他のトラフィックに一致する、または一致しないように指定する追加のルールを後で追加できます。

ルールを作成する場合は、インターネット宛ての適切なトラフィックに一致し、他の内部ネットワーク宛てのトラフィックには一致しないようにする方法を考慮します。たとえば、宛先が DMZ の内部サーバである場合に内部トラフィックがクラウド Web セキュリティに送信されないようにするには、DMZ へのトラフィックを免除する ACL に拒否 ACE を追加します。

**b.** [Source Criteria] 領域で、送信元 IP アドレスまたはネットワーク オブジェクト、オプションの IDFW ユーザ名またはグループ、および任意の TrustSec セキュリティ グループを入力または参照します。

**c.** [Destination Criteria] 領域で、宛先 IP アドレスまたはネットワーク オブジェクトおよび任意の TrustSec セキュリティ グループを入力または参照します。

FQDN ネットワーク オブジェクトは、特定のサーバへのトラフィックへの一致または除外に役立つ場合があります。

**d.** [Service] フィールドに、「http」または「https」を入力し、[Next] をクリックします。

**（注）** クラウド Web セキュリティは HTTP および HTTPS トラフィックだけで動作します。各トラフィックのタイプは、ASA によって個別に処理されます。このため、HTTP-only ルールおよび HTTPS-only ルールを作成する必要があります。

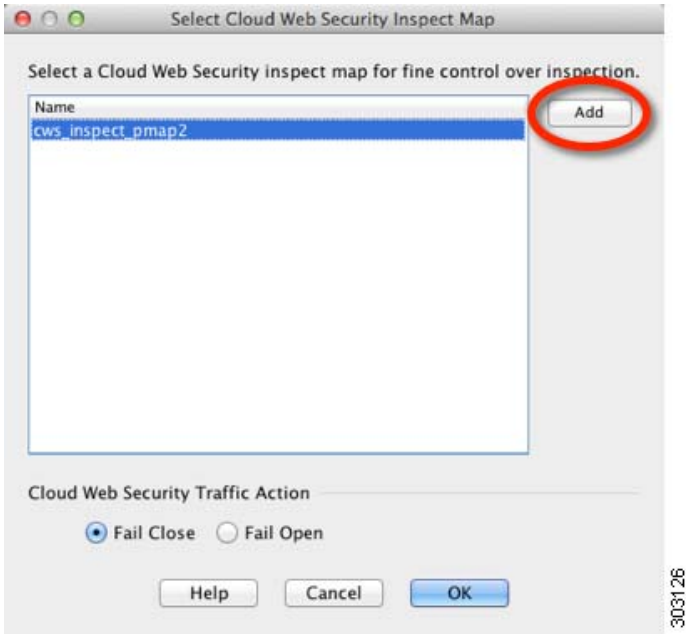
[Rule Actions] ダイアログボックスが表示されます。


**ステップ 4**　[Protocol Inspection] タブで、[Cloud Web Security] チェックボックスをオンにします。

**ステップ 5**　[Configure] をクリックし、トラフィック アクション（フェール オープンまたはフェール クローズ）を設定して、インスペクション ポリシー マップを追加します。

インスペクション ポリシー マップでは、ルールに不可欠なパラメータを設定し、任意で選択ホワイト リストを識別します。クラウド Web セキュリティに送信するトラフィックのクラスごとにインスペクション ポリシー マップが必要です。[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] ペインで、インスペクション ポリシー マップを事前に設定することもできます。

[Select Cloud Web Security Inspect Map] ダイアログボックスが表示されます。

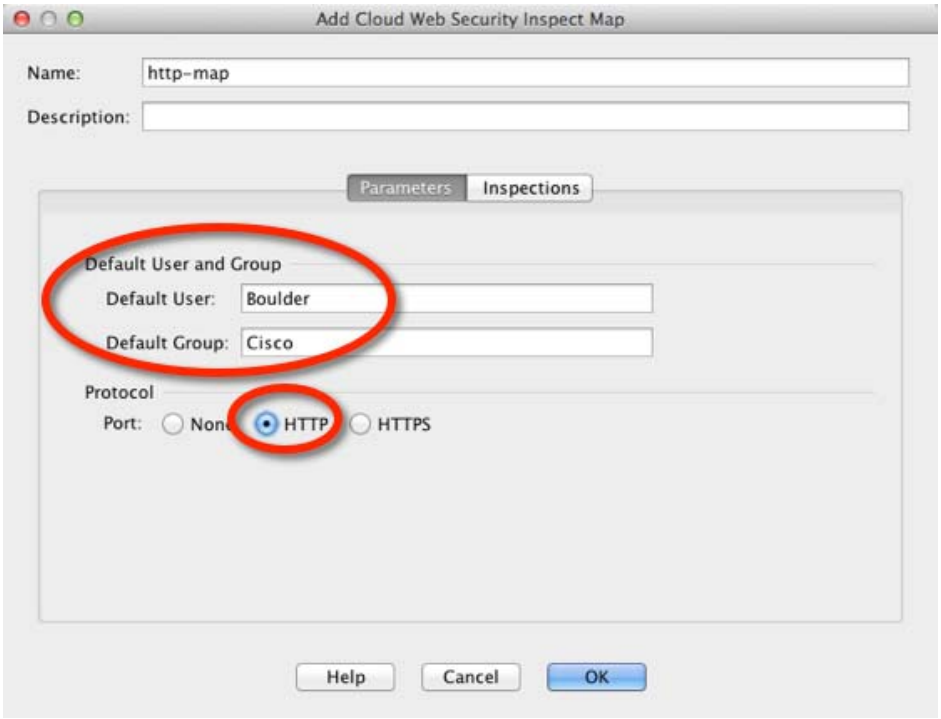



a. [Cloud Web Security Traffic Action] で、次のいずれかを選択します。
   - [Fail Close]：クラウド Web セキュリティ サーバを使用できない場合、すべてのトラフィックをドロップします。
   - [Fail Open]：クラウド Web セキュリティ サーバを使用できない場合、ASA を通過するトラフィックを許可します。

b. 既存のインスペクション ポリシー マップを選択するか、[Add] ボタンを使用して追加します。

c. [Add] をクリックして、新しいインスペクション ポリシー マップを追加します。

[Add Cloud Web Security Inspect Map] ダイアログボックスが表示されます。



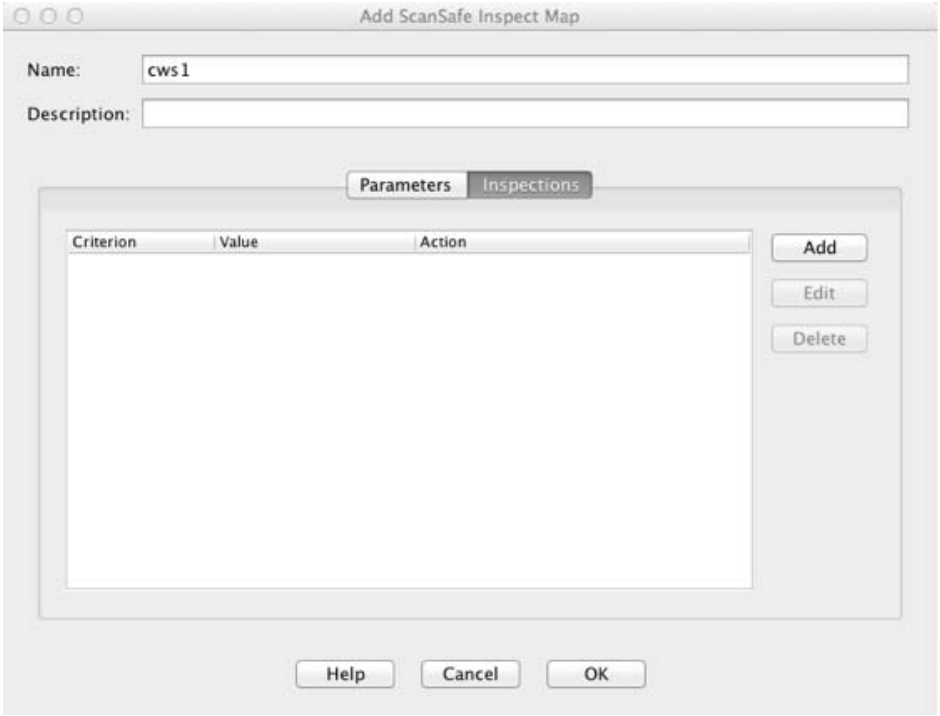

d. [Name] フィールドに、インスペクション ポリシー マップの名前を最大 40 文字までの長さで指定します。

e. （オプション）説明を入力します。

f. （オプション）[Parameters] タブで、[Default User] および [Default Group] を指定します。ASA が ASA に着信するユーザの ID を判定できない場合、デフォルト ユーザおよびグループが適用されます。

g. [Protocol] には、ステップ 3dで設定したサービスに一致する [HTTP] または [HTTPS] をクリックします。クラウド Web セキュリティは、各タイプのトラフィックを別々に処理します。

h. （オプション）ホワイト リストを識別するには、[Inspections] タブをクリックします。




- 「（オプション）ホワイトリストに記載されたトラフィックの設定　」（P.16-24）で作成したインスペクション クラス マップを選択するには、[Add] をクリックします。

  [Add Cloud Web Security Match Criterion] ダイアログボックスが表示されます。
- [Cloud Web Security Traffic Class] ドロップダウン メニューから、インスペクション クラス マップを選択します。

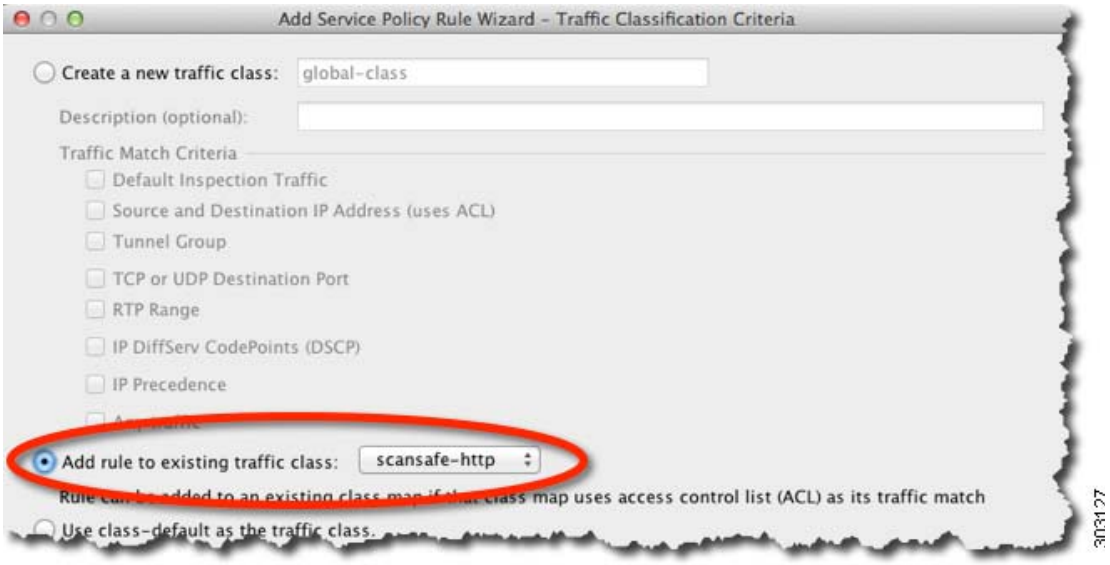
  クラス マップを追加または編集するには、[Manage] をクリックします。
- [Action] では、[Whitelist] をクリックします。
- ポリシー マップにホワイト リストを追加するには、[OK] をクリックします。
- [OK] をクリックします。

**ステップ 6**　[Finish] をクリックします。ルールは、サービス ポリシー ルール テーブルに追加されます。

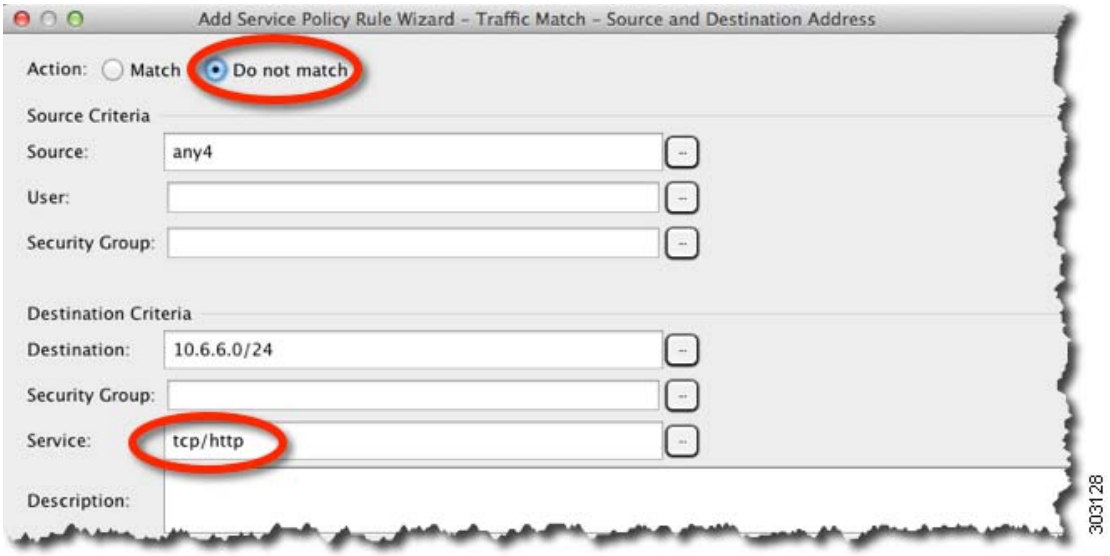
**ステップ 7**　追加のトラフィックを一致または除外するために、このトラフィック クラスに追加のサブルール（ACE）を追加するには、次の手順を実行します。

**a.** [Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。

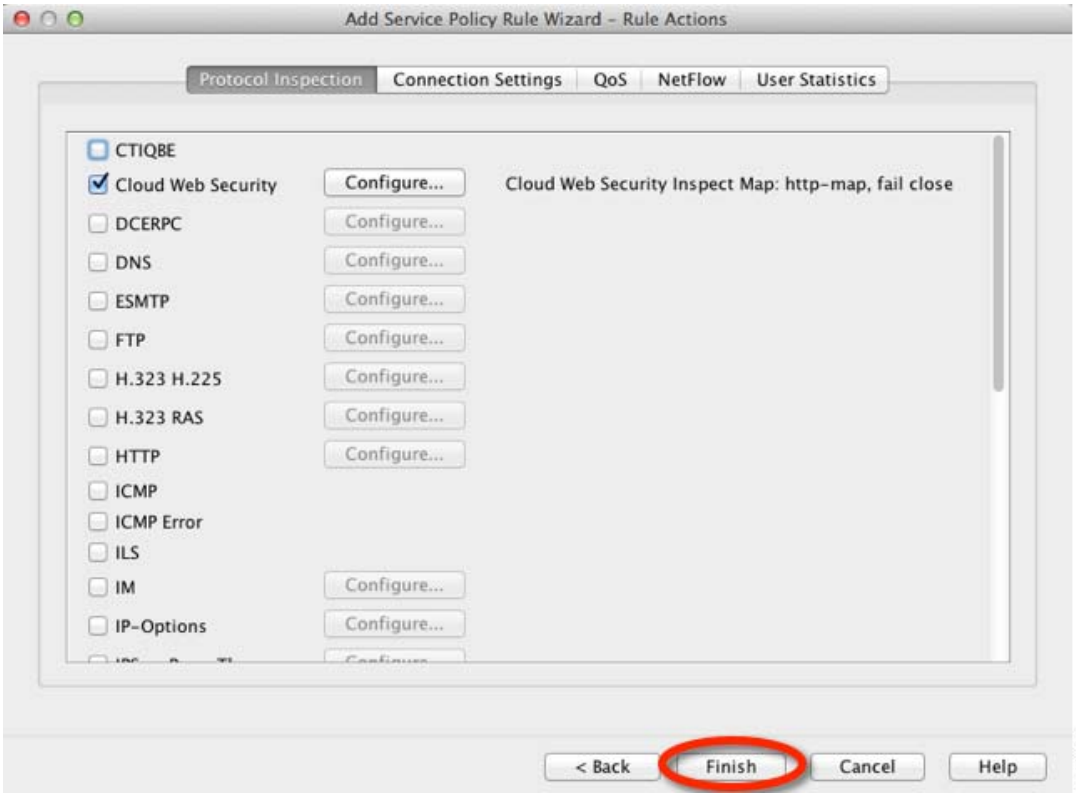
**b.** ステップ 2 で、同じサービス ポリシーを選択します。[Next] をクリックします。




c. [Traffic Classification Criteria] ダイアログボックスで、[Add Rule to Existing Traffic Class] を選択し、ステップ 3 で作成した名前を選択します。[Next] をクリックします。



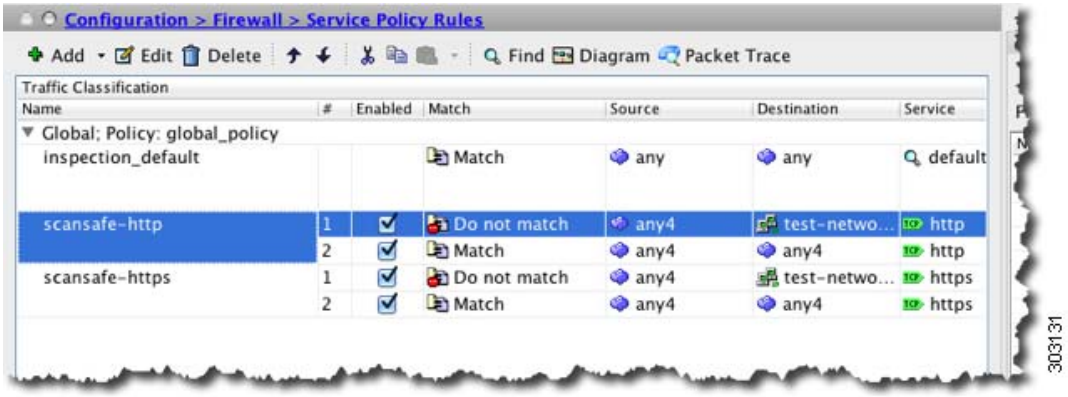

d. [Traffic Match - Source and Destination] ダイアログ ボックスで、[Match] を選択して追加トラフィックのインスペクションを追加するか、[Do Not Match] を選択してクラウド Web セキュリティ インスペクションからトラフィックを除外します。必ずこのクラス（HTTP または HTTPS）の前のルールに一致するようにサービスを設定してください。クラウド Web セキュリティの同じトラフィック クラスに HTTP と HTTPS を混在させることはできません。[Next] をクリックします。




e. [Rule Actions] ダイアログボックスでは、一切変更を加えずに [Finish] をクリックします。このトラフィック クラスでは、複数の ACE を追加した場合でも、1 セットのルールのアクションを使用できるので、すでに指定されているアクションは継承されます。

**ステップ 8**　HTTPS トラフィックなど、追加のトラフィック クラスを作成するには、この手順全体を繰り返します。ルールおよびサブルールを必要な数だけ作成できます。

**ステップ 9**　[Service Policy Rules] ペインでクラウド Web セキュリティのルールとサブルールの順序を調整します。ACE の順序の変更方法については、「サービス ポリシー ルールの順序の管理」（P.1-16）を参照してください。

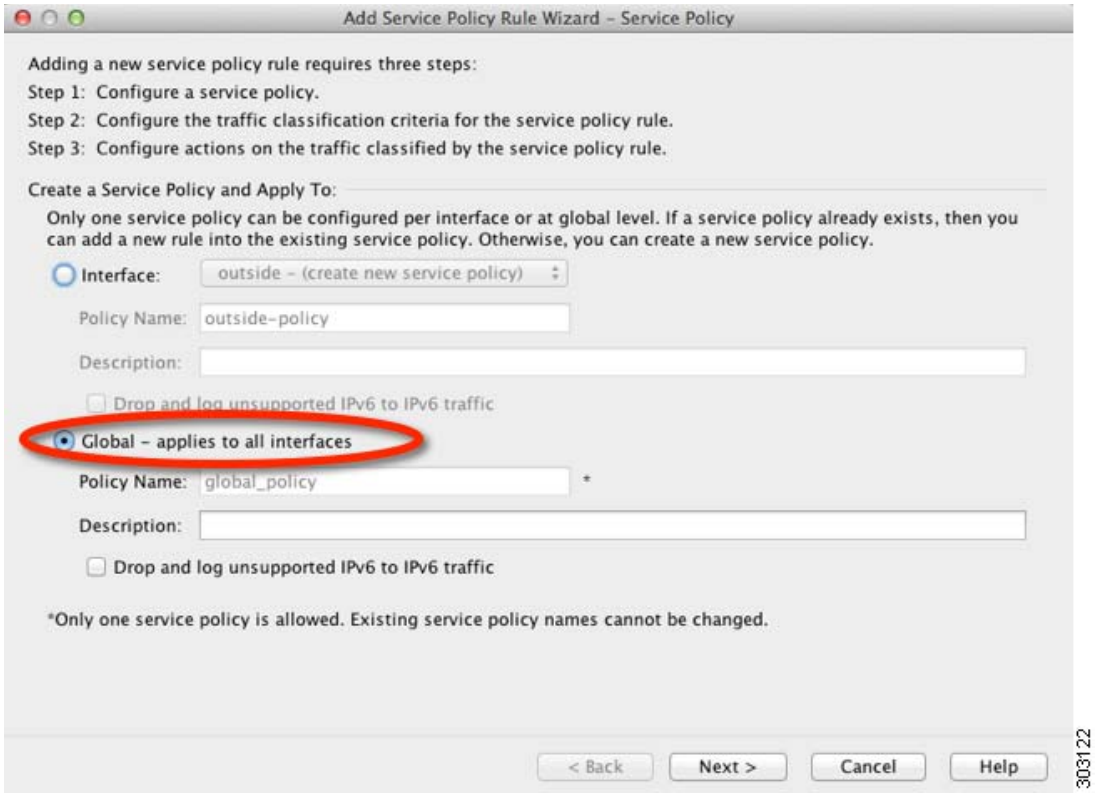



**ステップ 10**　[Apply] をクリックします。

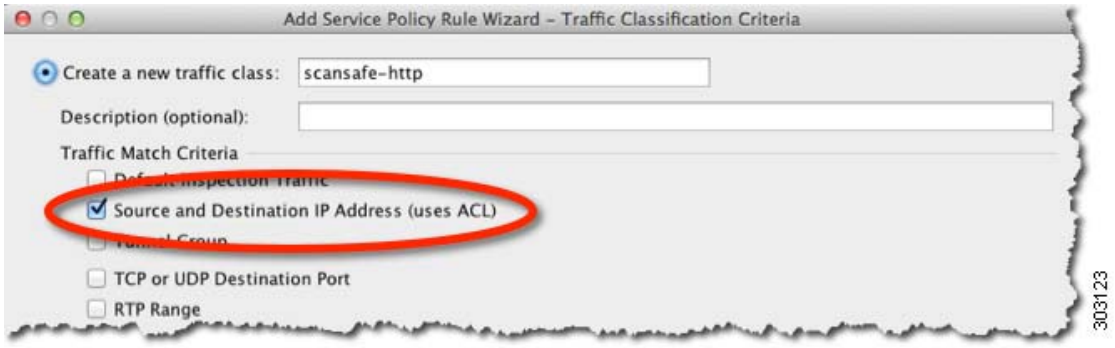
## 例

次の例は、10.6.6.0/24（test_network）に送信されるすべての IPv4 HTTP および HTTPS トラフィックを除外し、他のすべての HTTP および HTTPS トラフィックをクラウド Web セキュリティに送信し、このサービス ポリシー ルールを、既存のグローバル ポリシーの一部としてすべてのインターフェイスに適用します。クラウド Web セキュリティ サーバが到達不能の場合、ASA は一致するすべてのトラフィックをドロップします（フェール クローズ）。ユーザがユーザ ID 情報を持たない場合、デフォルトのユーザ Boulder とグループ Cisco が使用されます。

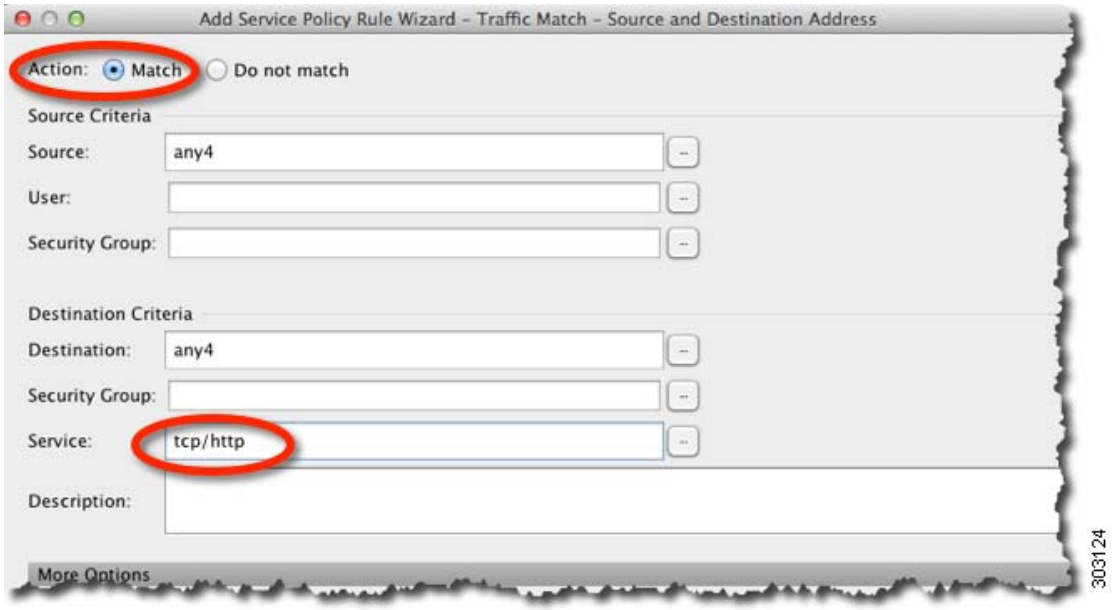
**ステップ 1**　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。デフォルトの global_policy にこのルールを追加します。




**ステップ 2**　「scansafe-http」と呼ばれる新しいトラフィック クラスを追加し、一致するトラフィックに ACL を指定します。

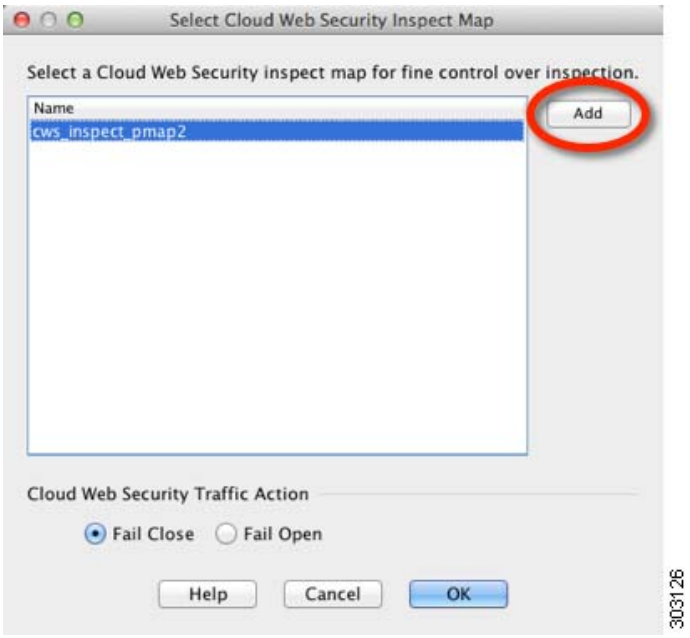



**ステップ 3**　[Match] を選択し、送信元と宛先に **any4** を指定します。サービスに **tcp/http** を指定します。

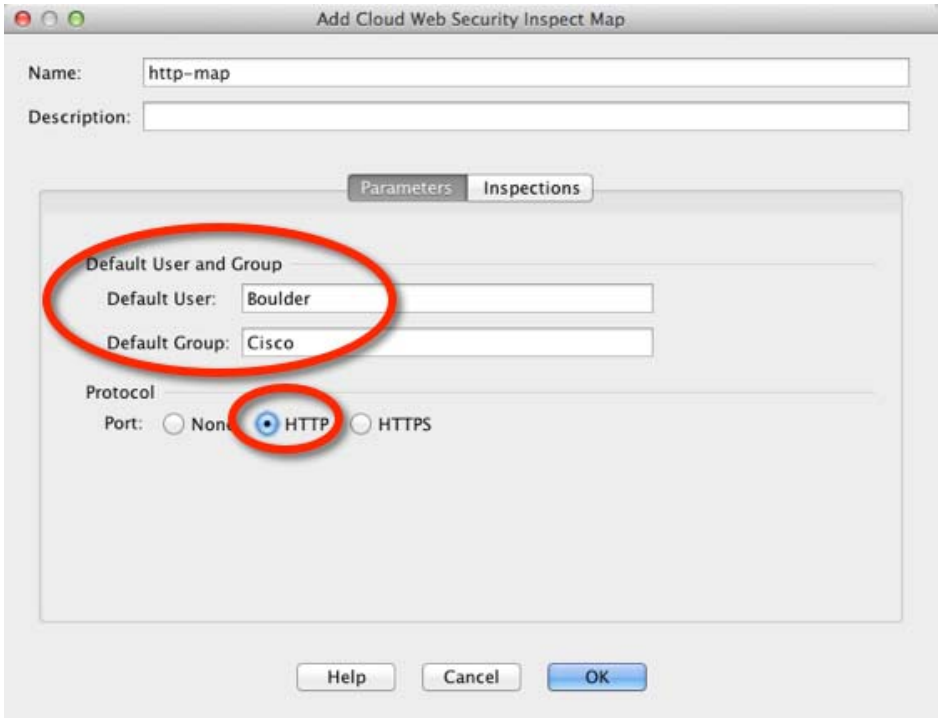



**ステップ 4**　[Cloud Web Security] をオンにして、[Configure] をクリックします。


**ステップ 5**　デフォルトの [Fail Close] アクションを受け入れ、[Add] をクリックします。

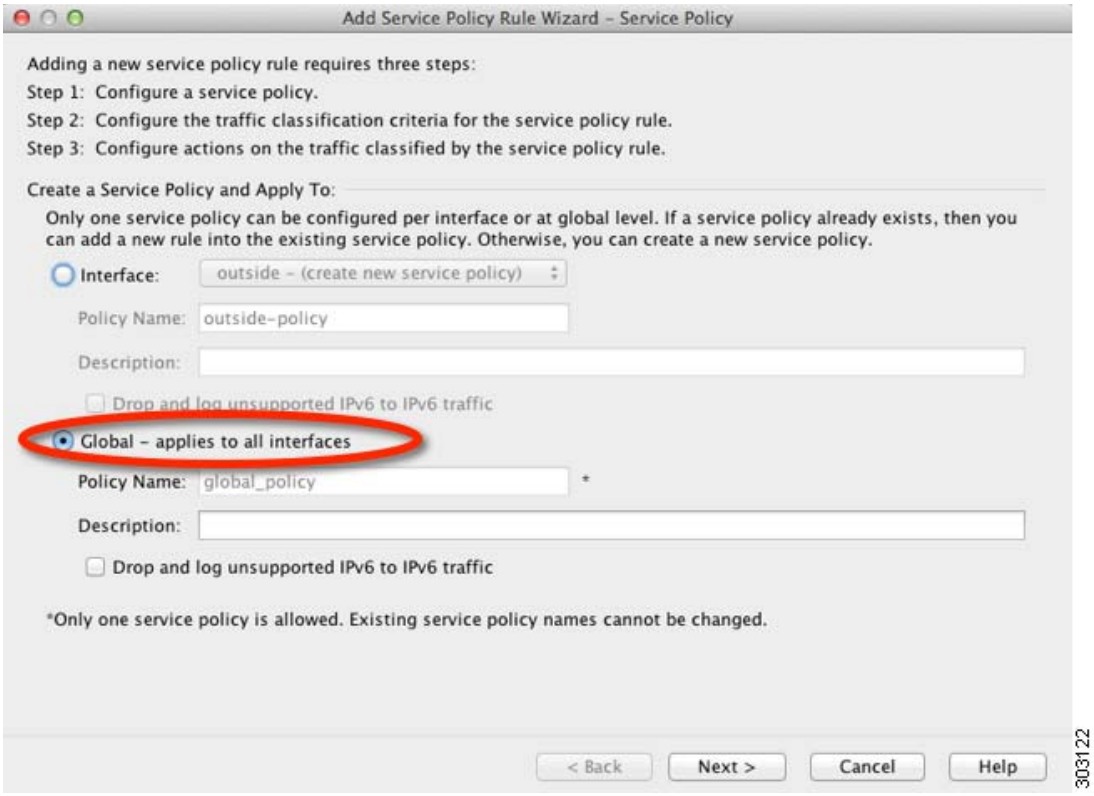



**ステップ 6**　インスペクション ポリシー マップに「http-map」という名前を付け、[Default User] に [Boulder]、[Default Group] に [Cisco] を設定します。[HTTP] を選択します。

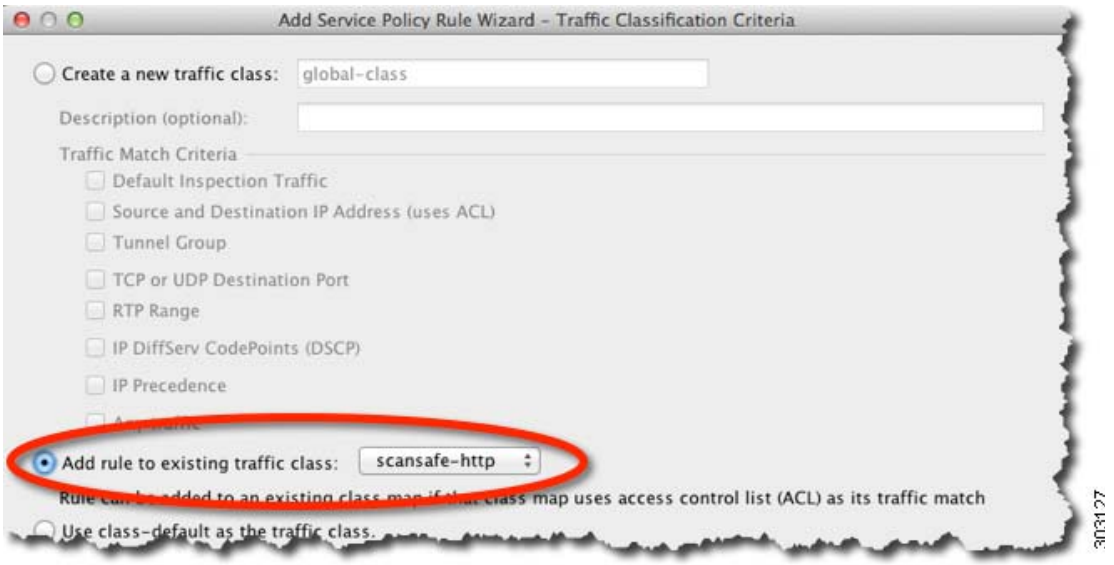



**ステップ 7**　[OK]、[OK] とクリックし、[Finish] をクリックします。ルールは、サービス ポリシー ルール テーブルに追加されます。

**ステップ 8**　[Configuration] > [Firewall] > [Service Policy Rules] を選択し、[Add] > [Service Policy Rule] をクリックします。デフォルトの global_policy に新しいルールを追加します。

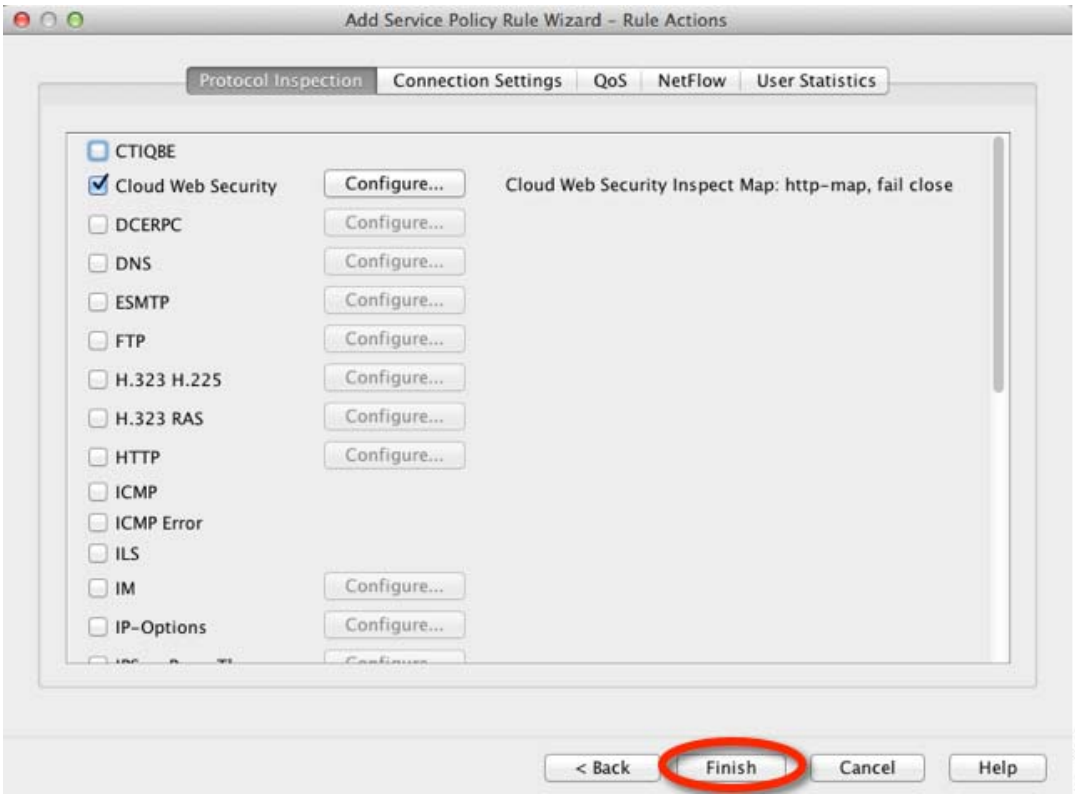



ステップ 9　[Add rule to existing traffic class] をクリックし、[scansafe-http] を選択します。




ステップ 10　[Do not match] を選択し、送信元として [any4]、宛先として [10.6.6.0/24] を設定します。[Service] を [tcp/http] に設定します。

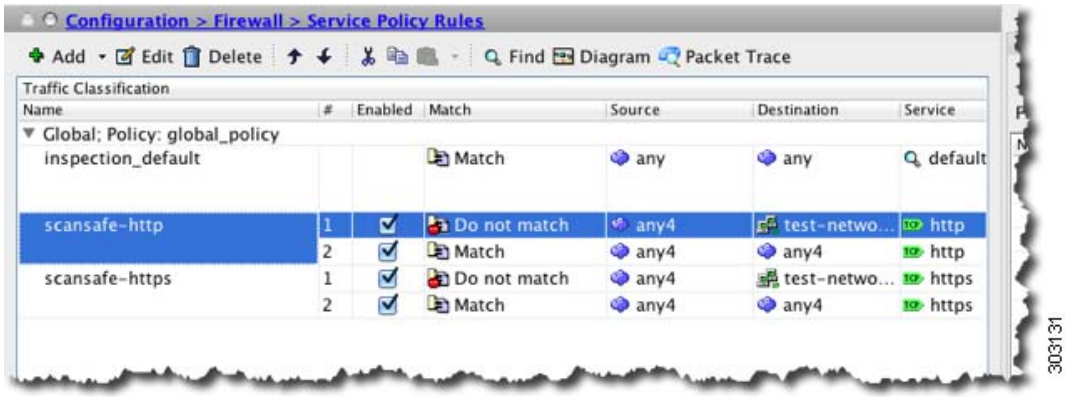

**ステップ 11**　[Finish] をクリックします。




**ステップ 12**　[Do not match] ルールが [Match] ルールの上に来るようにルールの順序を変更します。


ユーザ トラフィックは、これらのルールと順番に比較されます。この [Match] ルールはリストの最初にあるので、test_network へのトラフィックを含むすべてトラフィックがそのルールにのみ一致し、[Do not match] ルールがヒットすることはありません。[Do not match] ルールを [Match] ルールの上に移動すると、test_network へのトラフィックは [Do not match] に一致し、他のすべてのトラフィックは [Match] ルールに一致します。

**ステップ 13**　次のように変更して上記の手順を繰り返します。「scansafe-https」と呼ばれる新しいトラフィック クラスを追加し、インスペクション ポリシー マップに [HTTPS] を選択します。




**ステップ 14**　[Apply] をクリックします。

# （オプション）ホワイトリストに記載されたトラフィックの設定

ユーザ認証を使用する場合は、ユーザ名やグループ名に基づいて一部のトラフィックをクラウド Web セキュリティによるフィルタリングから免除できます。クラウド Web セキュリティ サービス ポリシー ルールを設定する場合は、ホワイトリスト インスペクション クラス マップを参照できます。IDFW および AAA のユーザ クレデンシャルをこの機能とともに使用できます。

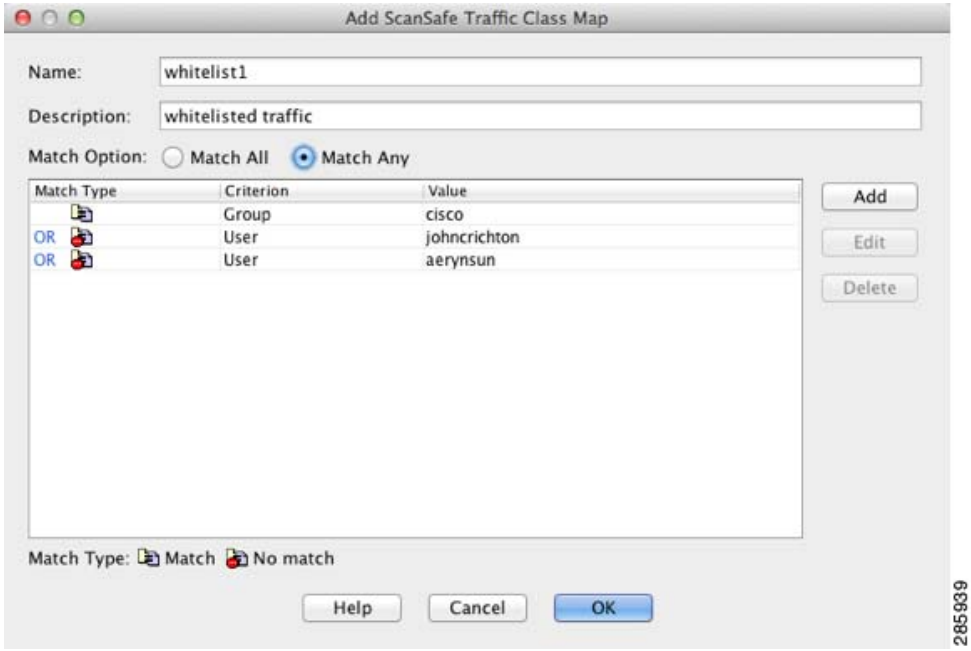
サービス ポリシー ルールを設定すると、ユーザまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

## 手順の詳細

**ステップ 1**　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security] を選択します。

**ステップ 2**　[Add] をクリックして、新しいクラス マップを作成します。

[Add Cloud Web Security Traffic Class Map] 画面が表示されます。




**ステップ 3**　[Name] フィールドに、新しいクラス マップの名前を入力します（40 文字以下）。

**ステップ 4**　[Description] フィールドに、クラス マップの説明を入力します（200 文字以下）。

**ステップ 5**　[Match Option] には、[Add] をクリックして定義した基準を選択します。

- [Match All]：トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。
- [Match Any]：トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。

**ステップ 6**　[Add] をクリックします。

[Add Cloud Web Security Match Criterion] ウィンドウが表示されます。

**ステップ 7**　[Match Type] を選択します。

- [Match]：ホワイト リストに任意のユーザ/グループを指定します。
- [No Match]：ホワイト リストに必要と*しない*ユーザ/グループを指定します。たとえば、ホワイト リストにグループ「cisco」を指定しているが、ユーザ「johncrichton」および「aerynsun」からのトラフィックはスキャンしたい場合、これらのユーザに [No Match] を指定することができます。

**ステップ 8**　[Match Criterion] を選択します。

- [User]：ユーザを指定します。
- [Group]：グループを指定します。
- [User and Group]：ユーザおよびグループを指定します。

**ステップ 9**　[OK] をクリックします。

**ステップ 10**　必要に応じてさらに一致基準を追加します。

**ステップ 11**　クラス マップを追加するには、[OK] をクリックします。

**ステップ 12**　[Apply] をクリックします。

**ステップ 13**　「クラウド Web セキュリティにトラフィックを送信するサービス ポリシーの方法」（P.16-10）に従って、クラウド Web セキュリティ ポリシーにホワイト リストを使用します。

# （オプション）ユーザ アイデンティティ モニタを設定します

IDFW を使用する場合、ASA は、アクティブな ACL に含まれるユーザおよびグループの AD サーバからのユーザ アイデンティティ情報のみをダウンロードします。ACL は、アクセス ルール、AAA ルール、サービス ポリシー ルール、またはアクティブと見なされるその他の機能で使用する必要があります。クラウド Web セキュリティでは、そのポリシーがユーザ アイデンティティに基づくことができるため、すべてのユーザに対する完全な IDFW カバレッジを取得するには、アクティブな ACL の一部ではないグループをダウンロードする必要があります。たとえば、ユーザおよびグループとともに ACL を使用するクラウド Web セキュリティ サービス ポリシー ルールを設定して、関連グループをアクティブ化できますが、これは必須ではありません。IP アドレスのみに基づく ACL を使用できます。ユーザ アイデンティティ モニタ機能を使用すると、AD エージェントからグループ情報を直接ダウンロードできます。

## 制限事項

ASA は、ユーザ アイデンティティ モニタ用に設定されたグループ、アクティブな ACL によってモニタされているグループも含めて 512 以下のグループモニタできます。

## 手順の詳細

**ステップ 1**　[Configuration] > [Firewall] > [Identity Options] を選択し、[Cloud Web Security Configuration] セクションにスクロールします。

**ステップ 2**　[Add] をクリックします。

[Add Monitor User] ダイアログボックスが表示されます。

**ステップ 3**　ドメインを追加するには、[Manage] をクリックして、[Add] をクリックします。ASA であらかじめ定義したドメインのグループのみモニタできます。

[Configure Identity Domains] ダイアログボックスが表示されます。ドメインを追加する方法の詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

**ステップ 4**　ドメインの追加が終了したら、[OK] をクリックします。

**ステップ 5**　グループ名を入力するか、またはドメインごとに AD エージェントのグループを検索できます。

- グループ名を直接入力するには、一番下のフィールドに次の形式で名前を入力し、[OK] をクリックします。

  *domain-name**group*

- AD エージェントのグループを検索するには、次の手順を実行します。

**a.**　[Domain] ドロップダウン リストからドメインを選択します。

b. [Find] フィールドで、グループ名に対応するテキスト文字列を入力し、[Find] をクリックします。

   ASA は、指定したドメインの AD エージェントから名前をダウンロードします。

c. モニタする名前をダブルクリックすると、一番下のフィールドに追加されます。

d. [OK] をクリックします。

追加グループに対して手順を繰り返します。

**ステップ 6**　モニタするグループを追加したら、[Apply] をクリックします。

# クラウド Web セキュリティ ポリシーの設定

ASA サービス ポリシー ルールを設定した後は、ScanCenter ポータルを起動して、Web コンテンツ スキャン、フィルタリング、マルウェア保護サービスおよびレポートを設定します。

### 手順の詳細

https://scancenter.scansafe.com/portal/admin/login.jsp に移動します。

詳細については、『Cisco ScanSafe Cloud Web Security Configuration Guides』を参照してください。

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

# クラウド Web セキュリティのモニタ

| コマンド | 目的 |
|---|---|
| [Monitoring] > [Properties] > [Cloud Web Security] | サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。<br>合計と現在の HTTP 接続を表示します。マルチ コンテキスト モードでは、統計情報はコンテキスト内にのみ表示されます。 |
| 次の URL を参照してください。<br>http://Whoami.scansafe.net | トラフィックがクラウド Web セキュリティ サーバに移動するかどうかを確認するには、クライアントからこの Web サイトにアクセスします。 |

# 関連資料

| 関連資料 | URL |
|---|---|
| 『Cisco ScanSafe Cloud Web Security Configuration Guides』 | http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html |

# Cisco クラウド Web セキュリティの機能の履歴

表 16-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

*表 16-1　クラウド Web セキュリティ の機能の履歴*

| 機能名 | プラットフォーム リリース | 機能情報 |
|---|---|---|
| クラウド Web セキュリティ | 9.0(1) | この機能が導入されました。<br>Cisco クラウド Web セキュリティ は、Web トラフィックに対するコンテンツ スキャンおよびその他のマルウェア保護サービスを提供します。また、ユーザ アイデンティティに基づいて Web トラフィックのリダイレクトと報告を行うこともできます。<br>次の画面が導入または変更されました。<br>[Configuration] > [Device Management] > [Cloud Web Security]<br>[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security]<br>[Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security] > [Add/Edit]<br>[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security]<br>[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] > [Add/Edit]<br>[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security] > [Add/Edit] > [Manage Cloud Web Security Class Maps]<br>[Configuration] > [Firewall] > [Identity Options]<br>[Configuration] > [Firewall] > [Service Policy Rules]<br>[Monitoring] > [Properties] > [Cloud Web Security] |