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（ScanSafe とも呼ばれる）では、Software as a Service（SaaS）モデルによる 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。

Cisco クラウド Web セキュリティに関する情報

ASA でクラウド Web セキュリティを有効にすると、ASA は、サービス ポリシー ルールに基づいて、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ます。これにより許容範囲での使用をユーザに促し、マルウェアから保護します。

ASA では、アイデンティティ ファイアウォールおよび AAA ルールによりユーザを認証および識別させることもできます（オプション）。ASA は、ユーザ クレデンシャル（ユーザ名およびユーザ グループを含む）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およびグループを指定できます。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のクラウド 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。

ユーザ アイデンティティおよびクラウド Web セキュリティ

ユーザアイデンティティを使用して、クラウド Web セキュリティでポリシーを適用できます。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。

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法をサポートします。

- アイデンティティ ファイアウォール：ASA が Active Directory（AD）でアイデンティティ ファイアウォールを使用すると、AD エージェントからユーザ名とグループが取得されます。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 のユーザおよびグループを使用するか、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たときに、ユーザ名およびグループが取得されます。
- 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。デフォルト グループを設定すると、これらのユーザがそのデフォルト グループに関連付けられます。AAA ルールの設定については、レガシー機能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：関連付けられたユーザ名またはグループがないトラフィックの場合、オプションのデフォルトのユーザ名およびグループ名を設定できます。これらのデフォルトは、クラウド Web セキュリティのサービス ポリシー ルールに一致するすべてのユーザに適用されます。

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**：同じ企業内の複数の ASA で企業認証キーを使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスを有効にします。
- **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 サービスを有効にします。
- 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。

ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこれらのキーを生成します。詳細については、次の URL にあるクラウド Web セキュリティのマニュアルを参照してください。

http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html

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、トラフィックを許可またはブロックしたり、ユーザに警告したりします。警告では、Web サイトに進むオプションがあります。

ASA ではなく、ScanCenter で URL フィルタリング ポリシーを設定します。

ただし、ポリシーの一部は、ポリシーが適用されるユーザに対するものです。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。グループ情報が ASA からリダイレクトされた要求に含まれているため、ASA から取得する可能性があるグループ情報の内容を理解する必要があります。

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。アイデンティティ ファイアウォールを使用する際、グループが存在する場合、グループはクライアントの HTTP 要求に含まれています。アイデンティティ ファイアウォール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。

ScanCenter では、ポリシーにディレクトリ 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。

- アイデンティティ ファイアウォール グループ名は次の形式で送信されます。

  *domain-name**group-name*

  ASA での形式は *domain-name**group-name* です。ただし、リダイレクトされた HTTP 要求にグループを含めるときに一般的な 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。
  - アイデンティティ ファイアウォール 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、デフォルトのユーザ名を「Guest」に設定すると、ASA は「Guest」を送信します。デフォルトのユーザ名を「Cisco\Guest」に設定すると、ASA は「Cisco\Guest」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。

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 Cloud Web Security サービスに登録すると、プライマリ Cloud Web Security 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 分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。ASA は、TCP スリーウェイ ハンドシェイクを完了するサーバの機能に基づいて可用性を判定します。

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。

クラウドWebセキュリティアプリケーションの状態をチェックすることで、フェールオーバーをさらに改善することができます。場合によっては、サーバが TCP スリーウェイ ハンドシェイクを完了できても、サーバ上のクラウド Web セキュリティ アプリケーションが正しく機能していないことがあります。アプリケーション健全性チェックを有効にすると、スリーウェイ ハンドシェイクが完了しても、アプリケーション自体が応答しない場合、システムはバックアップ サーバにフェールオーバーできます。これにより、より信頼性の高いフェールオーバー設定が確立されます。

ヘルス チェックでは、クラウド Web セキュリティ アプリケーションにテストの URL を使用して GET リクエストが送信されます。設定されているタイムアウト期限とリトライ限度内で応答に失敗すると、サーバはダウンとしてマーキングされ、システムはフェールオーバーを開始します。バックアップ サーバもまた、アクティブ サーバとしてマーキングされる前に、正しく機能していることを確認するためにテストされます。フェールオーバーの後、プライマリ サーバのアプリケーションは、オンラインに戻り再度アクティブ サーバとしてマーキングされるまで 30 秒ごとに再テストされます。

ASA がプライマリまたはバックアップのクラウド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。

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 セキュリティのガイドライン

フェールオーバーのガイドライン

フェールオーバー構成でサポートされます。ただし、アクティブ/アクティブ フェールオーバーでは、プライマリ ユニットでのみポリシーを設定します。クラウド Web セキュリティ コネクタはプライマリ ユニットからのみタワーの到達可能性を追跡します。セカンダリ ユニットはタワーを到達不能であるとして常に報告します。フェールオーバー時にセカンダリ ユニットがプライマリになると、セカンダリ ユニットがタワーの到達可能性を追跡できます。

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 コンテキスト内だけで使用でき、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。クラウド Web セキュリティ コネクタは、プライマリ管理コンテキストからのみタワーの到達可能性を追跡します。

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。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 を使用して、IPv6 アドレスを IPv4 に変換します。

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ていません。
- クラウド Web セキュリティは、URL フィルタリングも実行できるモジュール（ASA CX、ASA FirePOWER など）にリダイレクトする同じトラフィックでは使用できません。トラフィックは、クラウド Web セキュリティ サーバではなく、モジュールにのみ送信されます。
- 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。クライアントレス SSL VPN トラフィックについては、クラウド Web セキュリティの ASA サービス ポリシーの対象外となっていることを確認してください。
- 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、両方のサーバを表示します。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 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。
- 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。
- デフォルトのインスペクション トラフィック クラスには、クラウド Web セキュリティ インスペクション対応のデフォルト ポート（80 および 443）は含まれていません。

Cisco クラウド Web セキュリティの設定

クラウド Web セキュリティを設定する前に、使用するプロキシ サーバのライセンスおよびアドレスを取得します。さらに、認証キーを生成します。クラウド Web セキュリティの詳細については、http://www.cisco.com/go/cloudwebsecurity を参照してください。

Web トラフィックをクラウド Web セキュリティにリダイレクトするように ASA を設定するには、次のプロセスを使用します。

始める前に

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場合、ASA で次のいずれかを設定します。

- アイデンティティ ファイアウォール（ユーザ名とグループ）。
- AAA ルール（ユーザ名のみ）：レガシー機能ガイドを参照してください。

  www.example.com などの完全修飾ドメイン名（FQDN）を使用する場合は、ASA の DNS サーバを設定する必要があります。

手順

ステップ 1 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 （8 ページ）。
ステップ 2 （任意）ホワイトリストに記載されたトラフィックの識別 （10 ページ）。
ステップ 3 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 ポリシーの設定 （11 ページ）。
ステップ 4 （任意） ユーザ アイデンティティ モニタの設定 （17 ページ）
ステップ 5 クラウド Web セキュリティ ポリシーの設定 （18 ページ）。

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

ユーザ Web 要求を適切にリダイレクトできるようにクラウド Web セキュリティ プロキシ サーバを識別する必要があります。

マルチ コンテキスト モードでは、システム コンテキストでプロキシ サーバを設定してから、コンテキストごとにクラウド Web セキュリティをイネーブルにする必要があります。そのため、サービスを使用できるコンテキストもあれば、サービスを使用できないコンテキストもあります。

始める前に

- プロキシ サーバの完全修飾ドメイン名を使用するように ASA の DNS サーバを設定する必要があります。
- （マルチ コンテキスト モード）システム コンテキストと特定のコンテキストの両方のクラウド Web セキュリティ プロキシ サーバに対応するルートを設定する必要があります。これは、クラウド Web セキュリティ プロキシ サーバがアクティブ/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証します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Cloud Web Security]** を選択します。マルチコンテキスト モードでは、システム コンテキストでこれを行います。

ステップ 2 IP アドレスまたは完全修飾ドメイン名でプライマリおよびバックアップ サーバを識別します。

Cisco Cloud Web Security サービスに登録すると、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 サーバが割り当てられます。

デフォルトでは、クラウド Web セキュリティ プロキシ サーバは HTTP と HTTPS の両方のトラフィックにポート 8080 を使用します。指示されている場合以外は、この値を変更しないでください。

ステップ 3 （任意）[Health Check] グループで、フェールオーバー処理を向上させるために、アプリケーション健全性チェックを有効にします。

サーバが正常かどうかを判断する際に、クラウド Web セキュリティ アプリケーションの健全性をチェックするように Cisco クラウド Web セキュリティを設定できます。アプリケーションの健全性を確認することで、プライマリ サーバが TCP スリーウェイ ハンドシェイクに応答する場合に、システムはバックアップ サーバにフェールオーバーできますが、要求を処理することはできません。これにより、より信頼性の高いシステムを実現します。

次のオプションを設定します。

- [Application URL]：アプリケーションが対応可能かどうかを確認するためにシステムをポーリングするときに使用される URL。デフォルトの URL を使用するには、http://gs.scansafe.net/goldStandard?type=text&size=10 と入力します。その URL が必要とされるものでなくなった場合は、Cisco クラウド Web セキュリティから提供された新しい URL を指定します。
- [Application Timeout]：タイムアウトは、ヘルス チェック URL の GET リクエストの送信後に応答を取得するために ASA が待機する時間を決定します。ASA は、タイムアウト後にサーバのポーリングに対する再試行制限まで要求を再試行します。その後、サーバがダウンして、フェールオーバーが開始します。デフォルトは 15 秒で、範囲は 5 ～ 120 秒です。

ステップ 4 [Other] グループで、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。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] 、[Confirm License Key] ：要求の送信元の組織を示すため、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。認証キーは 16 バイトの 16 進数です。認証キーは 16 バイトの 16 進数です。

ステップ 5 [Apply] をクリックします。

ステップ 6 （マルチ コンテキスト モードのみ）サービスを使用する各コンテキストに切り替えてイネーブルにします。

任意で、コンテキストごとに別の認証キーを入力できます。認証キーが含まれていない場合は、システム コンテキストに設定された認証キーが使用されます。

ホワイトリストに記載されたトラフィックの識別

アイデンティティ ファイルまたはAAAルールを使用する場合、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。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。

ScanSafe インスペクション クラス マップでホワイトリストを設定します。アイデンティティ ファイルと AAA ルールの両方から取得されたユーザ名とグループ名を使用できます。IP アドレスまたは宛先 URL に基づいてホワイトリストに記載することはできません。

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、ポリシーのクラス マップを参照できます。サービス ポリシー ルールでトラフィック一致基準（ACL とともに）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。

手順

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

ステップ 2 次のいずれかを実行します。

- [Add] をクリックして、新しいクラスマップを追加します。マップ名（40 文字以下）を入力し、任意で説明を入力します。
- マップを選択して [Edit] をクリックします。

ステップ 3 照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。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] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

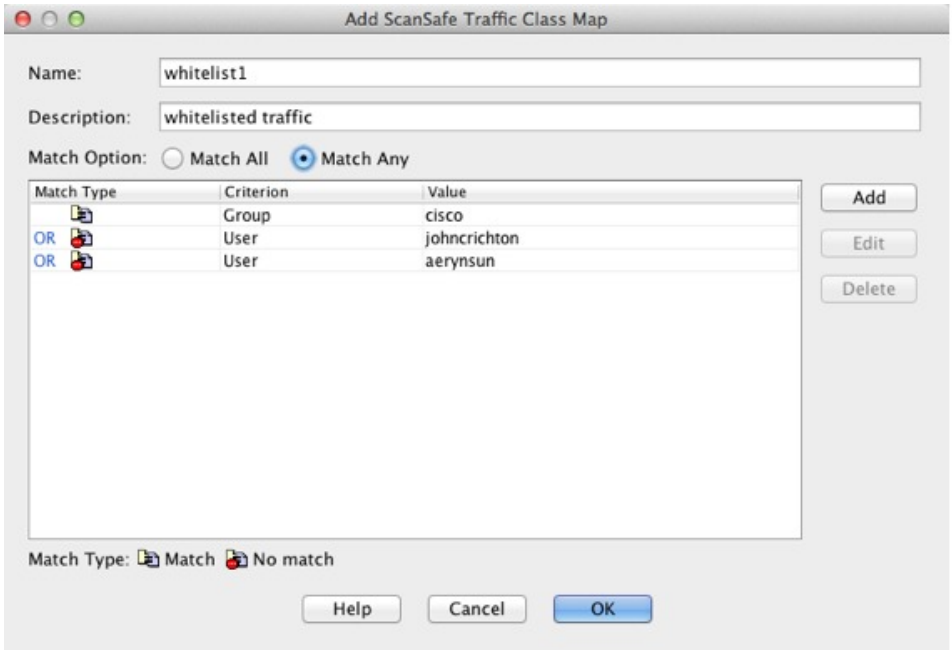
ステップ 4 一致テーブルのエントリを追加または編集して、一致基準を設定します。ターゲットのトラフィックを定義するために必要なものをすべて追加します。

a) 基準の一致タイプの（[Match] または [No Match]）を選択します。

- [Match]：ホワイト リストに任意のユーザまたは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または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。

b) ユーザまたはグループ、あるいはその両方を定義しているかどうかを選択し、ユーザまたはグループの名前を入力します。

c) [OK] をクリックします。ホワイトリストのすべての基準を追加するまで、このプロセスを繰り返します。



ステップ 5 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 6 [Apply] をクリックします。

これで、クラウド Web セキュリティ サービス ポリシーでホワイトリストを使用できます。

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 ポリシーの設定

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。

始める前に

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、最初にホワイトリストを作成します。

手順

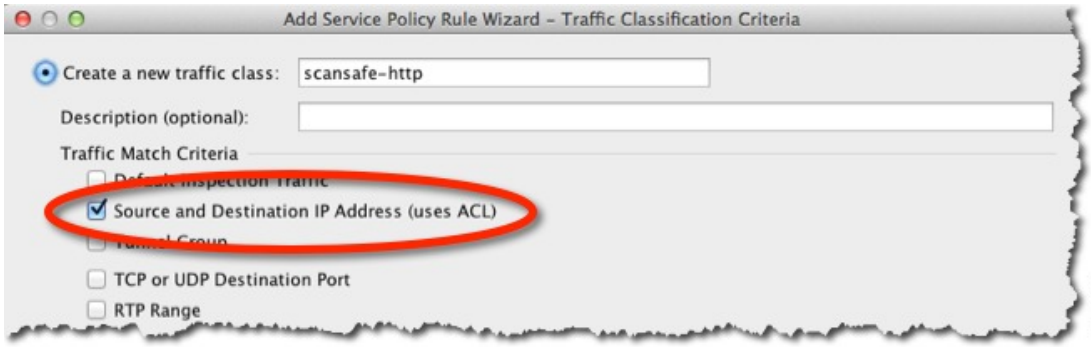
ステップ 1 **[Configuration]** > **[Firewall]** > **[Service Policy]** を選択して、ルールを開きます。

- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。ポリシーを追加すると、そのポリシーを特定のインターフェイスに適用したり、すべてのインターフェイスにグローバルに適用したりすることができます。インターフェイスにすでにグローバル ポリシーやポリシーがある場合は、既存のポリシーにルールを追加していることになります。新しいルールに名前を付けることができます。[Next] をクリックして続行します。
- ScanSafe インスペクション ルールがある場合、または ScanSafe インスペクションを追加するルールがある場合、それを選択し、[Edit] をクリックします。[Global] フォルダの「inspection_default」ルールには、HTTP および HTTPS ポートが含まれていないため、そのルールに ScanSafe インスペクションを追加できないことに注意してください。

ステップ 2 [Traffic Classification Criteria] ページで、次のいずれかのオプションを選択してポリシー アクションを適用するトラフィックを指定し、[Next] をクリックします。新しいクラスを作成する際、クラスにわかりやすい名前を付けてください。さらに、HTTP と HTTPS のトラフィックに対して別々のクラスを作成する必要があることに注意してください。

- [Create a new traffic class] > [Source and Destination IP Address （uses ACL）] : クラウド Web セキュリティにトラフィック クラスがまだない場合は、ACL マッチングがクラスを定義する最も柔軟な方法であるため、このオプションを推奨します。

  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 [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。



- [Create a new traffic class] > [TCP or UDP Port]：Web トラフィックを区別しない場合は、このオプションを使用します。[Next] をクリックして、1 つのポート（**TCP http** または **TCP https**）を指定します。
- [Add rule to existing traffic class] ：すでに Cisco クラウド Web セキュリティ インスペクションの ACL を開始しており、ルールを既存のポリシーに追加する場合は、このオプションを選択してトラフィック クラスを選択します。

ステップ 3 （ACL マッチング）送信元と宛先の基準に基づいてトラフィック クラスを定義する場合、このルールの ACL 属性を入力します。

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。

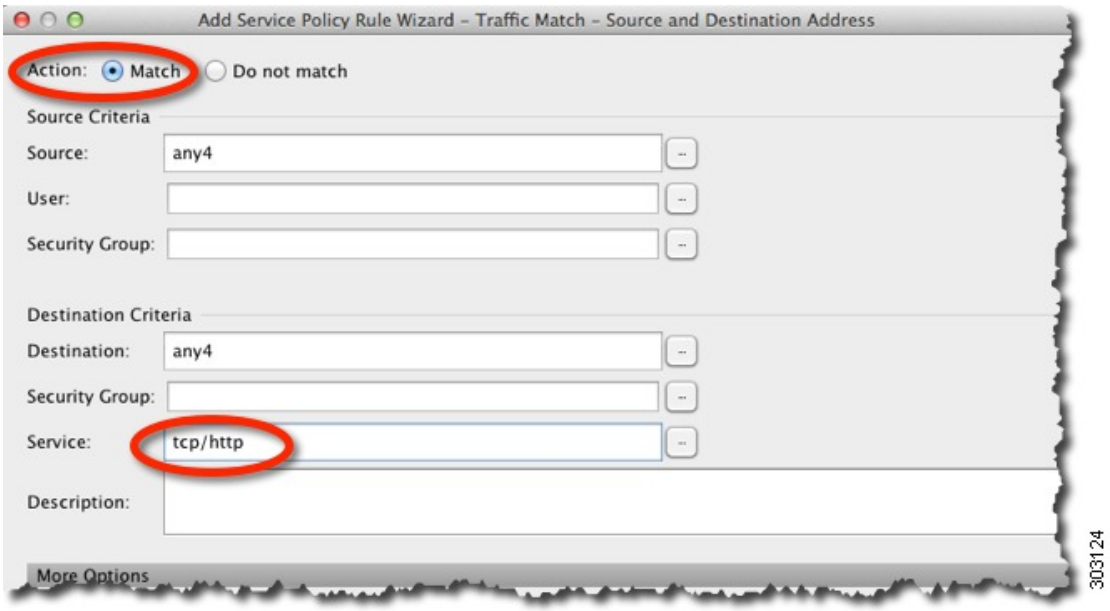
b) [Source Criteria] 領域で、送信元 IP アドレスまたはネットワーク オブジェクトを入力または参照します。また、アイデンティティ ファイアウォールのユーザ引数と Cisco Trustsec セキュリティ グループを使用して、トラフィックを識別できるようにすることも可能です。クラウド Web セキュリティに TrustSec セキュリティ グループ情報を送信しないことに注意してください。セキュリティ グループに基づいてポリシーを定義できません。

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。



ステップ 4 [Rule Actions] ページの [Protocol Inspection] タブで、[Cloud Web Security] チェック ボックスをオンにします。

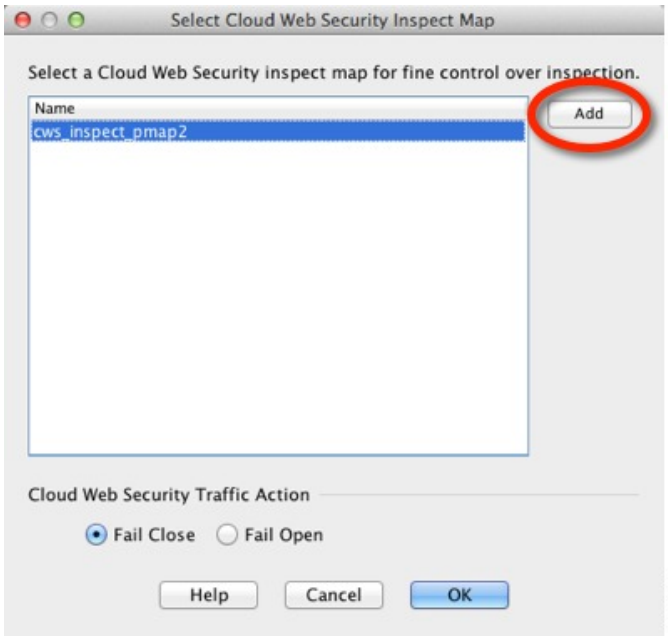
ステップ 5 [Configure] をクリックし、トラフィック アクションを設定して、インスペクション ポリシー マップを追加します。

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] を選択して、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。

a) [Cloud Web Security Traffic Action] で、次のいずれかを選択します。

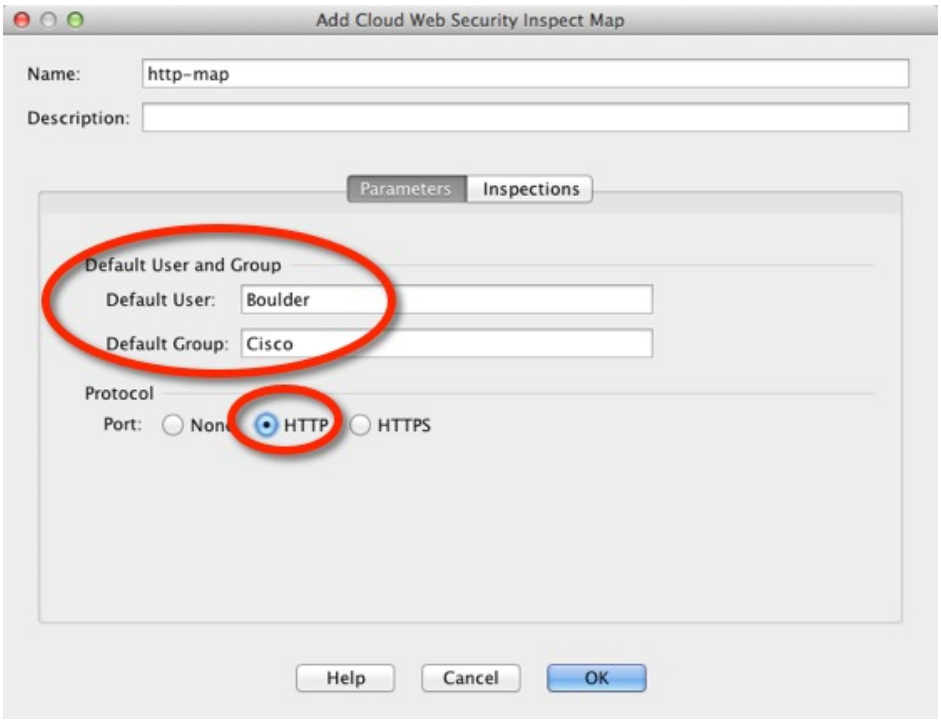
- [Fail Close] ：クラウド Web セキュリティ サーバを使用できない場合、すべてのトラフィックをドロップします。
- [Fail Open] ：クラウド Web セキュリティ サーバを使用できない場合、ASA を通過するトラフィックを許可します。

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] をクリックして新しいマップを追加します。



c) （新しいマップのみ）[Cloud Web Security Inspection Map] ダイアログボックスで、マップの名前を入力して次の属性を設定します。完了したら、[OK] をクリックします。

- [Default User and Group]：（任意）デフォルトのユーザまたはグループ名、あるいはその両方。ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合、デフォルトのユーザやグループがクラウド Web セキュリティに送信される HTTP 要求に含まれます。このユーザ名またはグループ名に対して ScanCenter のポリシーを定義できます。
- [Protocol]：トラフィック クラスで選択したサービスに基づいて [HTTP] または [HTTPS] を選択します。これらの選択は一致している必要があります。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。



- [Inspections] タブ：（任意）ホワイトリストを識別するには、[Inspections] タブの [Add] をクリックしてホワイトリストのクラス マップを選択します。また、この時点で [Manage] をクリックして、ホワイトリストを追加することもできます。アクションとして [Whitelist] が選択されていることを確認し、[OK] をクリックします。追加のホワイトリストを追加できます。

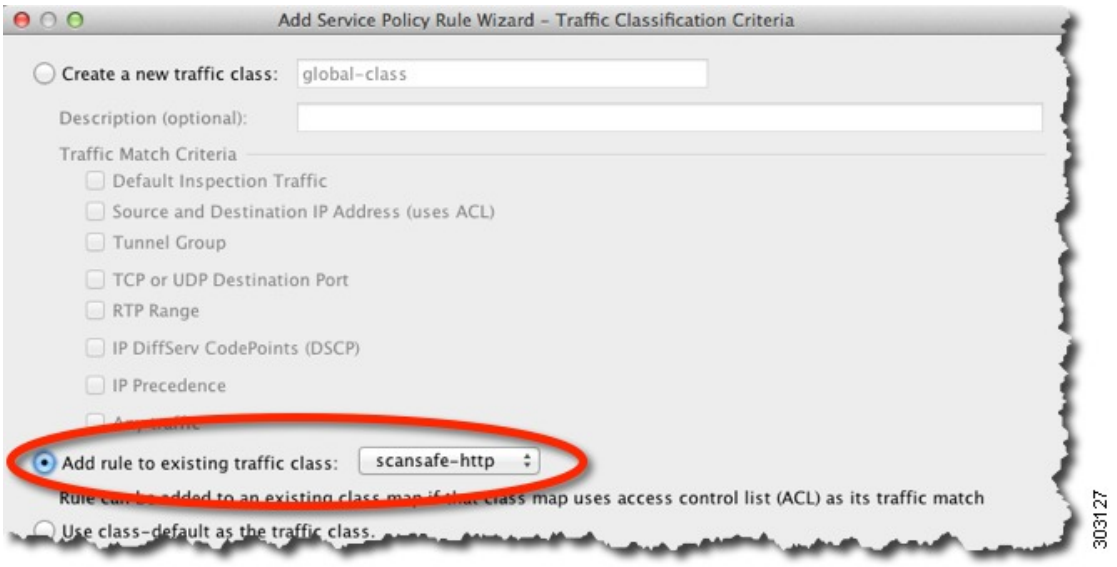
d) [Select Cloud Web Security Inspect Map] ダイアログ ボックスの [OK] をクリックします。

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、このプロセスを繰り返して同じインターフェイスまたはグローバル ポリシーを選択します。トラフィック クラスを設定する際、[Add rule to existing traffic class] オプションを選択し、クラウド Web セキュリティ クラスを選択します。

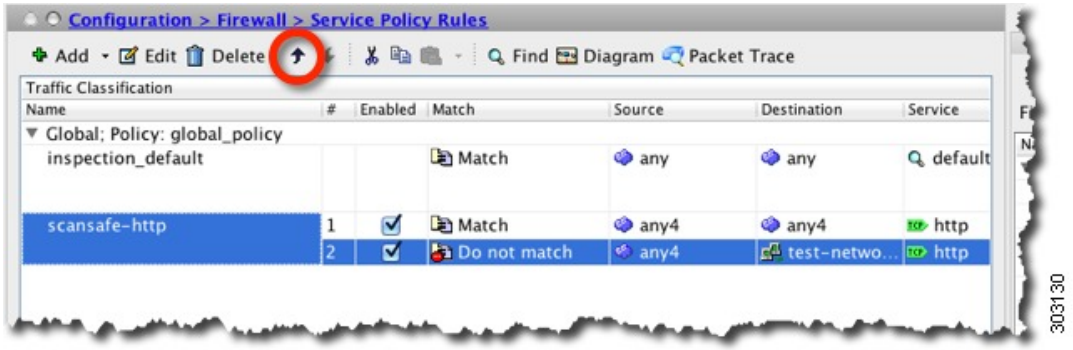
新しい ACE を設定する場合、クラス内の他のルールで使用されるのと同じサービス（HTTP または HTTPS）を指定してください。

[Rule Actions] ページの変更は行わないでください。ルールが完了したら、[Finish] をクリックします。



ステップ 8 HTTPS トラフィック（HTTP トラフィック クラスから開始したと仮定した場合）など、他のプロトコルのトラフィック 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。移動するルールを選択して、上下ボタンをクリックします。特定のルールがより一般的なルールよりも前に配置されていることを確認します。



ステップ 10 [Apply] をクリックします。

ユーザ アイデンティティ モニタの設定

アイデンティティ ファイアウォールを使用する場合、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。

たとえば、ユーザおよびグループを含む ACL を使用するようにクラウド Web セキュリティ サービス ポリシー ルールを設定し、関連する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。

クラウド Web セキュリティでは、その ScanCenter 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アイデンティティ ファイアウォール 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ことが必要な場合があります。ユーザアイデンティティモニタでは、ADエージェントからグループ情報を直接ダウンロードすることができます。

（注） 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

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。

ステップ 3 グループが含まれているドメインを選択してから、ユーザ グループ リストでグループをダブルクリックし、[OK] をクリックします。このプロセスを繰り返してグループを追加します。

- 多数のグループがある場合は、[Find] ボックスを使用してリストをフィルタ処理します。ASA は、指定したドメインの AD から名前をダウンロードします。
- また、*domain_name**group_name* の形式でグループ名を直接入力することもできます。
- 必要に応じて、[Manage] ボタンをクリックして新しいドメインを追加できます。

ステップ 4 モニタするすべての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。

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

クラウド Web セキュリティをモニタするには、[Monitoring] > [Properties] > [Cloud Web Security] を選択します。このページには、リダイレクトされた HTTP/HTTPS 接続のプロキシ サーバのステータスおよび統計情報が表示されます。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。

クライアント マシンから次の URL にアクセスして、ユーザのトラフィックがプロキシ サーバにリダイレクトされているかどうかを判断できます。ページに、ユーザが現在サービスを使用しているかどうかを示すメッセージが表示されます。

http://Whoami.scansafe.net

Cisco クラウド Web セキュリティの例

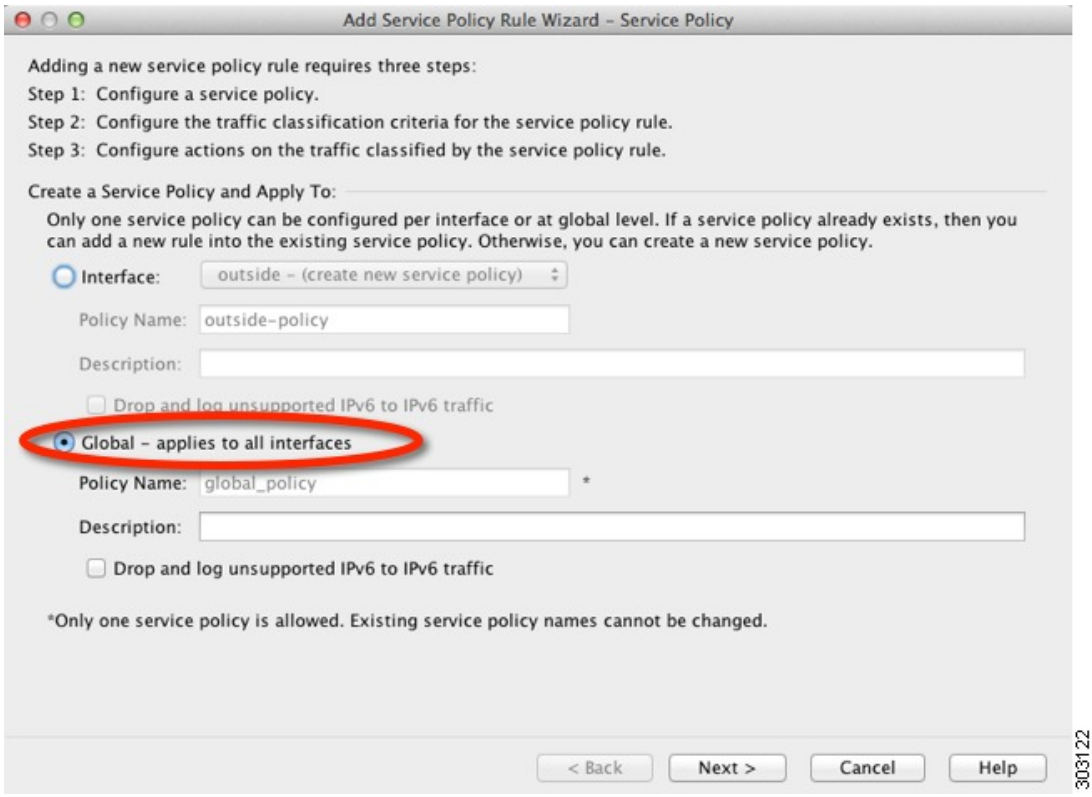
次に、クラウド Web セキュリティの設定例をいくつか示します。

クラウド Web セキュリティ用のサービス ポリシーの例

次の例は、10.6.6.0/24 ネットワーク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）。ユーザにユーザ ID 情報がない場合、デフォルトのユーザ Boulder とグループ Cisco が使用されます。

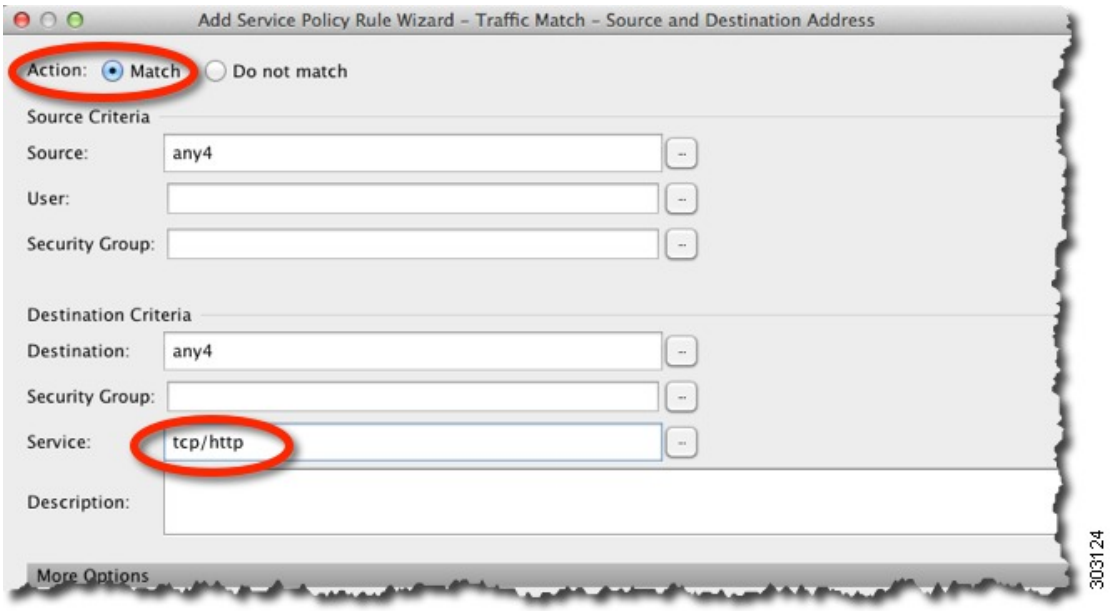
手順

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。[Next] をクリックします。



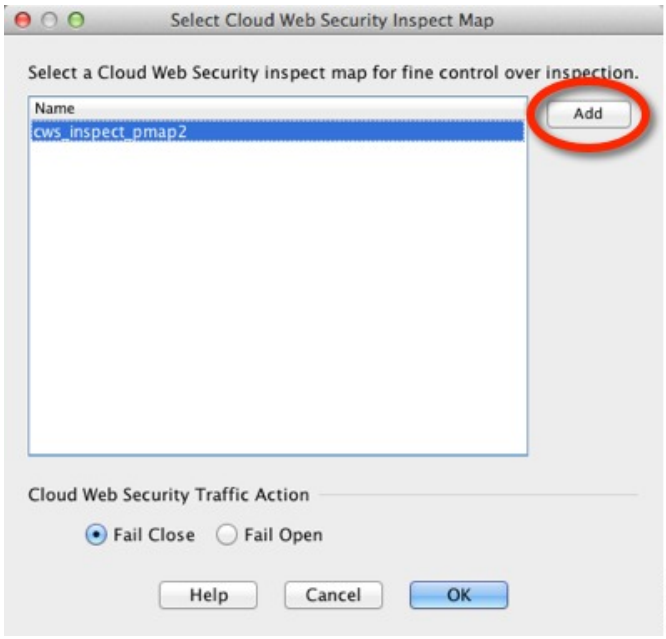
ステップ 2 「scansafe-http」と呼ばれる新しいトラフィック クラスを追加し、一致するトラフィックに ACL を指定します。[Next] をクリックします。

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。[Next] をクリックします。

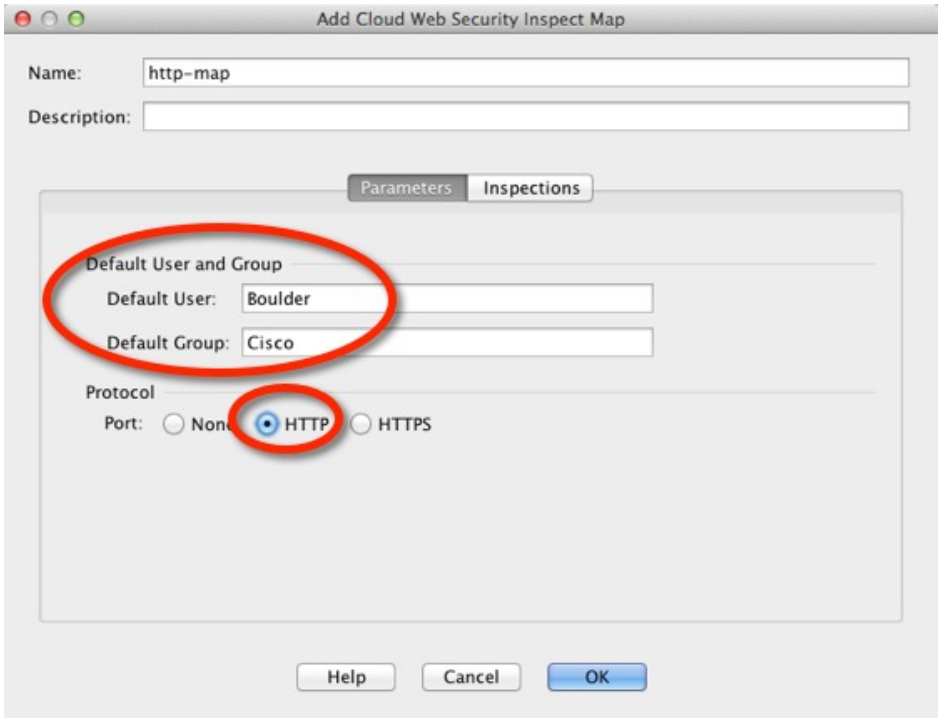


ステップ 4 [Protocol Inspection] タブの [Cloud Web Security] をオンにして、[Configure] をクリックします。

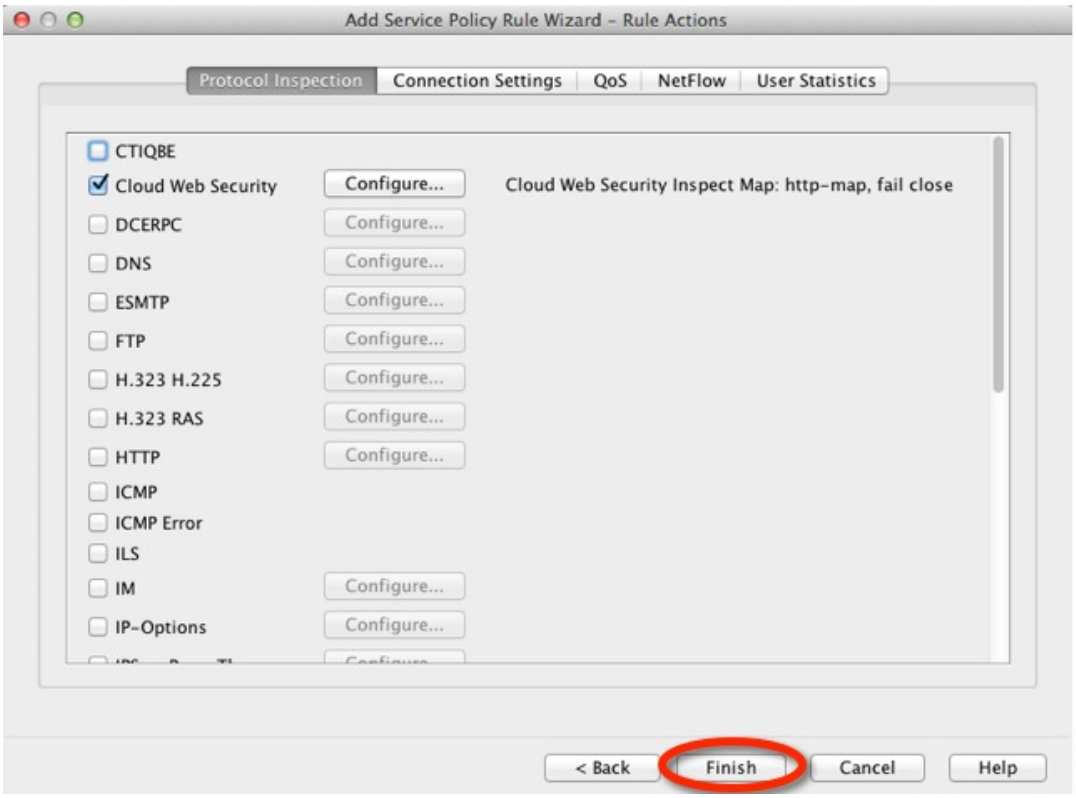
ステップ 5 デフォルトの [Fail Close] アクションを受け入れ、[Add] をクリックします。



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。

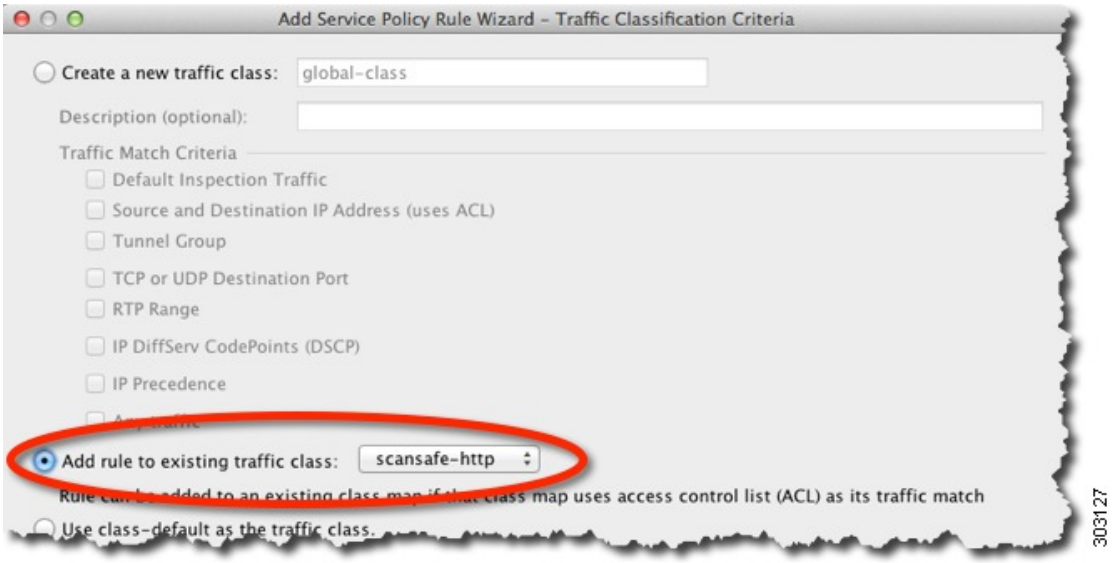


ステップ 7 [OK]、[OK] とクリックし、[Finish] をクリックします。 ルールは、サービス ポリシー ルール テーブルに追加されます。

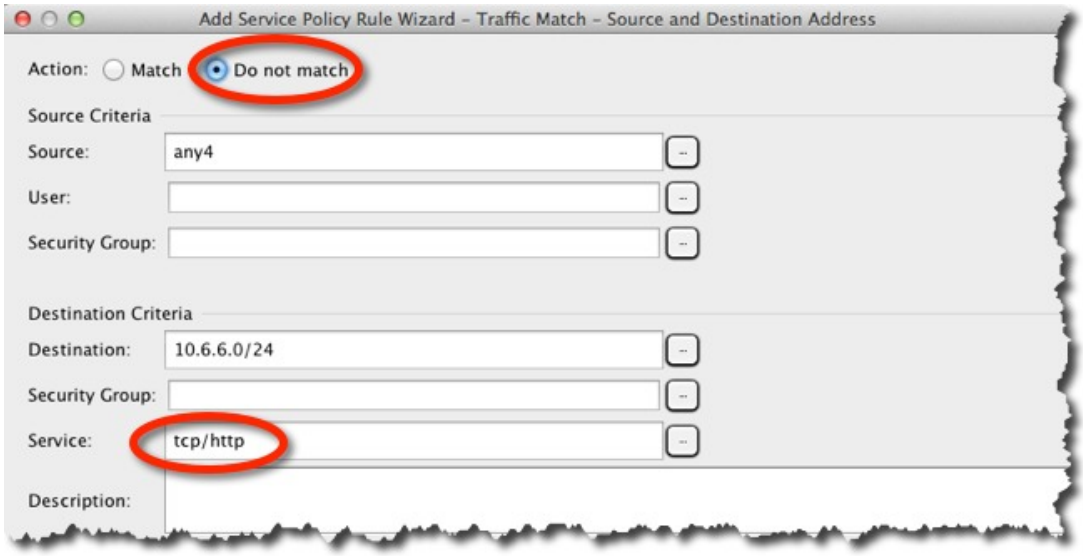


ステップ 8 **[Configuration]** > **[Firewall]** > **[Service Policy Rules]** を選択し、**[Add]** > **[Service Policy Rule]** をクリックします。デフォルトの global_policy に新しいルールを追加して [Next] をクリックします。

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。[次へ（Next）] をクリックします。

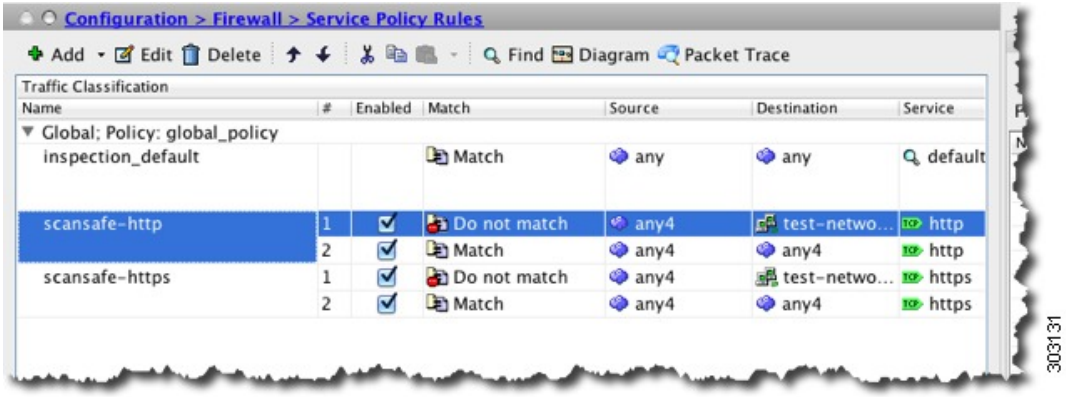


ステップ 11 [完了（Finish）] をクリックします。

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、テスト ネットワーク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、テスト ネットワーク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。

Cisco クラウド Web セキュリティの履歴

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。 Cisco クラウド Web セキュリティは、Web トラフィックに対してコンテンツ スキャンなどのマルウェア防御サービスを実行します。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。 次の画面が導入または変更されました。 [Configuration] > [Device Management] > [Cloud Web Security Configuration] > [Firewall] > [Objects] > [Class Maps] > [Cloud Web Security Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [Cloud Web Security Configuration] > [Firewall] > [Identity Options Configuration] > [Firewall] > [Service Policy Rules Monitoring] > [Properties] > [Cloud Web Security]

機能名	プラットフォーム リリース	機能情報
Cisco クラウド Web セキュリティのアプリケーション層健全性チェック。	9.6(2)	サーバが正常かどうかを判断する際に、クラウド Web セキュリティ アプリケーションの健全性をチェックするように Cisco クラウド Web セキュリティを設定できるようになりました。アプリケーションの健全性を確認することで、プライマリ サーバが TCP スリーウェイ ハンドシェイクに応答する場合に、システムはバックアップ サーバにフェールオーバーできますが、要求を処理することはできません。これにより、より信頼性の高いシステムを実現します。 **[Configuration] > [Device Management] > [Cloud Web Security]** の画面が変更されました。