Web セキュリティの設定

Web セキュリティ モジュールについて

AnyConnect Web セキュリティ モジュールは、HTTP トラフィックを Cisco Cloud Web Security スキャニング プロキシにルーティングするエンドポイント コンポーネントです。

同時に各要素を分析できるように、Cisco Cloud Web Security は Web ページの要素を分解します。たとえば、特定の Web ページが HTTP、Flash、および Java 要素の組み合わせである場合、別個の「scanlets」がこれらの各要素を並行して分析します。次に、Cisco Cloud Web Security は、Cisco ScanCenter 管理ポータルに定義されたセキュリティ ポリシーに基づいて、良性または受け入れ可能なコンテンツを許可し、悪意があるか受け入れられないコンテンツをドロップします。これは、少数のコンテンツが許容されないために Web ページ全体が制限される「過剰ブロック」、または許容されないか場合によっては有害なコンテンツがページで提供されているのにページ全体が許可される「不十分なブロック」を防止します。Cisco Cloud Web Security は、社内ネットワークに接続しているかどうかにかかわらずユーザを保護します。

多数の Cisco Cloud Web Security スキャニング プロキシが世界各国に普及することで、AnyConnect Web セキュリティを活用するユーザは、遅延を最小限に抑えるために、応答時間が最も早い Cisco Cloud Web Security スキャニング プロキシにトラフィックをルーティングできます。

社内 LAN 上にあるエンドポイントを識別するように Secure Trusted Network Detection 機能を設定できます。この機能が有効になっている場合、社内 LAN から発信されるすべてのネットワーク トラフィックは、Cisco Cloud Web Security スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、Cisco Cloud Web Security ではなく、社内 LAN 上のデバイスにより別の方法で管理されます。

AnyConnect Web セキュリティ機能は、AnyConnect プロファイル エディタにより編集する AnyConnect Web セキュリティ クライアント プロファイルを使用して設定されます。

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。Cisco ScanCenter を使用して作成または設定されたコンポーネントの一部は、AnyConnect Web セキュリティ クライアント プロファイルにも組み込まれています。

（注） ISE サーバは、静的な例外リストに常に記載されている必要があります。このリストは、Web セキュリティ クライアント プロファイルの [例外（Exceptions）] ペインに設定されています。

一般的な Web セキュリティの設定

手順

ステップ 1 クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシを設定します。

ステップ 2 （任意）Cisco Cloud Web Security スキャニング プロキシについて、プロファイル エディタ内の既存のリストと、http://www.scansafe.cisco.com/ Web サイトからダウンロードしたスキャニング プロキシのリストを比較して相違がある場合、スキャニング プロキシ リストの更新を実行します。

ステップ 3 （任意）ユーザに対するスキャニング プロキシの表示または非表示を設定します。

ステップ 4 デフォルトのスキャニング プロキシの選択を行います。

ステップ 5 （任意）HTTP(S) トラフィック リスニング ポートの指定を行って、HTTPS Web トラフィックをフィルタリングします。

ステップ 6 Web スキャニング サービスでのエンドポイント トラフィックの除外または包含に対して、ホスト、プロキシ、または静的な例外を設定します。この設定により、指定された IP アドレスからのネットワーク トラフィックの評価が制限されます。

ステップ 7 ユーザ制御の設定および最も早いスキャニング プロキシ応答時間の計算を行います。この設定により、ユーザが接続する Cisco Cloud Web Security スキャニング プロキシが選択されます。

ステップ 8 社内 LAN から発信されるネットワーク トラフィックが Cisco Cloud Web Security スキャニング プロキシをバイパスするようにするには、Secure Trusted Network Detection の使用します。

ステップ 9 認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信を行います。この設定により、企業ドメイン、Cisco ScanCenter または Active Directory グループに基づいてユーザが認証されます。

クライアント プロファイルでの Cisco Cloud Web Security スキャニング プロキシ

Cisco Cloud Web Security は、Web コンテンツを分析して、セキュリティ ポリシーに基づいて良性コンテンツの提供をブラウザに許可し、悪意のあるコンテンツをブロックします。スキャ

ニング プロキシは、Cisco Cloud Web Security が Web コンテンツを分析する Cisco Cloud Web セキュリティ プロキシ サーバです。AnyConnect Web セキュリティ プロファイル エディタ内の [スキャニング プロキシ（Scanning Proxy）] パネルは、AnyConnect Web セキュリティ モジュールによる Web ネットワーク トラフィックの送信先 Cisco Cloud Web Security スキャニング プロキシを定義します。

IPv6 Web トラフィックのガイドライン

IPv6アドレス、ドメイン名、アドレス範囲、またはワイルドカードの例外が指定されている場合を除き、IPv6 Web トラフィックはスキャニング プロキシに送信されます。スキャニング プロキシは、DNS ルックアップを実行して、ユーザが到達しようとしている URL の IPv4 アドレスがあるかどうかを確認します。IPv4 アドレスが見つかると、スキャニング プロキシはこのアドレスを使用して接続します。IPv4 アドレスが見つからない場合、接続はドロップされます。

すべての IPv6 トラフィックがスキャニング プロキシをバイパスできるようにするには、すべての IPv6 トラフィックに静的な例外 ::/0 を追加します。この例外により、すべての IPv6 トラフィックがすべてのスキャニング プロキシをバイパスします。したがって、IPv6 トラフィックは Web セキュリティで保護されません。

（注） Windows が実行されているコンピュータでは、AnyConnect がユーザ ID を判別できない場合、内部 IP アドレスがユーザ ID として使用されます。たとえば、enterprise_domains プロファイル エントリが指定されていない場合、内部 IP アドレスを使用して、Cisco ScanCenter でレポートを生成します。

Mac OS X が実行されているコンピュータでは、Mac がドメインにバインドされている場合、Webセキュリティモジュールは、コンピュータがログインしているドメインを報告できます。ドメインにバインドされていない場合、Web セキュリティ モジュールは、Mac の IP アドレスまたは現在ログインしているユーザ名を報告できます。

ユーザがスキャニング プロキシを選択する方法

プロファイルの設定方法に応じて、ユーザがスキャニング プロキシを選択できるか、または AnyConnect Web セキュリティ モジュールが応答時間が最も早いスキャニング プロキシにユーザを接続します。

- クライアント プロファイルがユーザ制御を許可した場合、ユーザは Cisco AnyConnect Secure Mobility Client Web Security トレイの [設定（Settings）] タブからスキャン プロキシを選択できます。
- クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] 設定が有効になっている場合、AnyConnect Web セキュリティは、スキャニング プロキシを速い順に順序付けし、応答時間が最も速いスキャニング プロキシにユーザを接続します。
- クライアント プロファイルでユーザ制御が許可されなくても、[スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が有効になっているときは、AnyConnect Web

セキュリティは、ユーザをデフォルトのスキャニング プロキシから、応答時間が最も速いスキャニング プロキシに切り替えます（応答時間が、最初に接続したデフォルトのスキャニング プロキシよりも大幅に速い場合）。

- ユーザが、現在のスキャニング プロキシからローミングし始めたときに、クライアント プロファイルで [スキャン プロキシの自動選択（Automatic Scanning Proxy Selection）] が設定されていれば、AnyConnect Web セキュリティは、ユーザを新しいスキャニング プロキシに切り替えます（応答時間が現在のスキャニング プロキシよりも大幅に早い場合）。

AnyConnect Web セキュリティでは、Windows の拡張された AnyConnect トレイ アイコン、AnyConnect GUI の [詳細設定（Advanced Settings）] タブ、および [詳細統計情報（Advanced Statistics）] タブに有効になっているスキャニング プロキシ名が表示されるため、ユーザは接続先のスキャニング プロキシを確認できます。

スキャニング プロキシ リストの更新

Web セキュリティ プロファイル エディタのスキャニング プロキシ リストは編集不可能です。Cisco Cloud Web Security スキャニング プロキシを Web セキュリティ プロファイル エディタ内のテーブルで追加したり削除したりすることはできません。

Web セキュリティ プロファイル エディタを起動した後で、スキャニング プロキシの最新のリストが保持されている Cisco Cloud Web Security Web サイトにアクセスすることで、スキャニング プロキシ リストが自動的に更新されます。

AnyConnect Web セキュリティ クライアント プロファイルの追加または編集時に、プロファイル エディタは、Cisco Cloud Web Security スキャニング プロキシの既存のリストを、http://www.scansafe.cisco.com/ からダウンロードされたスキャニング プロキシ リストと比較します。リストが古い場合は、「スキャニング プロキシ リストが古くなっています（Scanning Proxy list is out of date）」というメッセージと [リストの更新（Update List）] と表示されたコマンド ボタンが表示されます。スキャニング プロキシ リストを、Cisco Cloud Web Security スキャニング プロキシの最新のリストで更新するには、[リストの更新（Update List）] をクリックします。

[リストの更新（Update List）] をクリックすると、プロファイル エディタによって、既存の設定が可能な限り保持されます。プロファイル エディタは、デフォルト スキャニング プロキシの設定、および既存の Cisco Cloud Web Security スキャニング プロキシの表示または非表示設定を保持しています。

ユーザに対するスキャニング プロキシの表示または非表示

ユーザが ASA への VPN 接続を確立した後で、ASA は、クライアント プロファイルをエンドポイントにダウンロードします。AnyConnect Web セキュリティ クライアント プロファイルは、ユーザに表示される Cisco Cloud Web Security スキャニング プロキシを判別します。

ローミング ユーザが最大の利点を得るには、すべての Cisco Cloud Web Security スキャニング プロキシをすべてのユーザに表示することをお勧めします。

ユーザは、次の方法で、AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ リストで「Display」とマークされたスキャニング プロキシと対話します。

- Cisco Cloud Web Security スキャニング プロキシは、Cisco AnyConnect Secure Mobility Client インターフェイスの [Web セキュリティ（Web Security）] パネルの [詳細（Advanced）] 設定のユーザに表示されます。
- AnyConnect Web セキュリティ モジュールは、応答時間でスキャニング プロキシを順序付ける際に、「Display」とマークされた Cisco Cloud Web Security スキャニング プロキシをテストします。
- ユーザは、自分のプロファイルでユーザ制御が許可される場合に接続する Cisco Cloud Web Security スキャニング プロキシを選択できます。
- AnyConnect Web セキュリティ クライアント プロファイルのスキャニング プロキシ テーブルで「Hide」とマークされている Cisco Cloud Web Security スキャニング プロキシは、ユーザに表示されず、応答時間でスキャニング プロキシを順序付ける際に評価されません。ユーザは、「Hide」とマークされたスキャニング プロキシには接続できません。

始める前に

AnyConnect Web セキュリティ クライアント プロファイルを作成します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 Cisco Cloud Web Security スキャニング プロキシをユーザに非表示または表示するには、次の手順を実行します。

- 非表示にするスキャニング プロキシを選択し、[非表示（Hide）] をクリックします。
- 表示するスキャニング プロキシの名前を選択し、[表示（Display）] をクリックします。すべての Cisco Cloud Web Security スキャニング プロキシを表示するよう設定することをお勧めします。

ステップ 4 AnyConnect Web セキュリティ クライアント プロファイルを保存します。

デフォルトのスキャニング プロキシの選択

ユーザが初めてネットワークに接続すると、デフォルトのスキャニング プロキシにルーティングされます。デフォルトでは、作成するプロファイルには、次の Cisco Cloud Web Security スキャニング プロキシ属性があります。

- スキャニング プロキシ リストには、ユーザがアクセス可能なすべての Cisco Cloud Web Security スキャニング プロキシが入力されています。これらはすべて [表示（Display）] とマークされています。
- デフォルトの Cisco Cloud Web Security スキャニング プロキシは事前選択されています。
- AnyConnect Web セキュリティ モジュールが HTTP トラフィックを受信するポートのリストには、いくつかのポートが設定されています。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [デフォルトのスキャニング プロキシ（Default Scanning Proxy）] フィールドからデフォルトのスキャニング プロキシを選択します。

ステップ 4 AnyConnect Web セキュリティ クライアント プロファイルを保存します。

HTTP(S) トラフィック リスニング ポートの指定

Scan Safe Web スキャニング サービスは、デフォルトで HTTP Web トラフィックを分析します。設定を通じて、HTTPS Web トラフィックをフィルタリングできます。Web セキュリティ クライアント プロファイルで、Web セキュリティがこれらのタイプのネットワーク トラフィックをリッスンするポートを指定します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [トラフィック リスニング ポート（Traffic Listen Port）] フィールドに、Web セキュリティ モジュールが HTTP トラフィック、HTTPS トラフィック、または両方をリッスンする論理ポート番号を入力します。

ステップ 4 Web セキュリティ クライアント プロファイルを保存します。

パブリック プロキシを設定するための Windows インターネット オプションの設定

通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。パブリック プロキシ サーバは認証プロキシ サーバと呼ばれます。このサーバにはユーザ名とパスワードが必要となることがあります。AnyConnect Web セキュリティでは、基本と NTLM という 2 種類の認証がサポートされています。プロキシ サーバが認証必須に設定されている場合、AnyConnect Web セキュリティは実行時にプロキシを検出し、認証プロセスを管理します。プロキシ サーバへの認証に成功すると、AnyConnect Web セキュリティが、Web トラフィックをパブリック プロキシ経由で Cisco クラウド Web セキュリティ スキャン プロキシへルーティングします。AnyConnect Web セキュリティはプロキシのクレデンシャルを暗号化してメモリ内に安全にキャッシュします。ユーザがプロキシ ネットワークから非プロキシ ネットワークに移動し、再びこのプロキシネットワークに戻る場合でも、クレデンシャルが再び必要となることがありません。パブリック プロキシを使用する場合、サービスの再起動は不要です。ユーザが非プロキシ ネットワークに移動すると、AnyConnect Web セキュリティは実行時にこれを自動的に検出し、Cisco クラウド Web セキュリティ スキャン プロキシに Web トラフィックを直接送信開始します。

Windows のインターネット オプションで、クライアント側でパブリック プロキシを使用するように設定されている場合、AnyConnect はその接続を使用します。

（注） Windows では基本および NTLM パブリック プロキシがサポートされています。Mac では基本パブリック プロキシだけがサポートされています。

1. Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。
2. [接続（Connections）] タブを選択し、[LANの設定（LAN Settings）] をクリックします。
3. プロキシ サーバを使用するように LAN を設定します。

4. プロキシ サーバの IP アドレスまたはホスト名を入力します。FTP/HTTP/HTTPS に対してそれぞれ個別のプロキシが設定されている場合は、HTTPSプロキシだけが考慮されます。

制限事項

- パブリック プロキシの背後にある IPv6 および TND はサポートされません。
- プロキシ IP は、AnyConnect Web セキュリティの例外リストに含まれていてはなりません。例外リストに含まれている場合、トラフィックが AnyConnect Web セキュリティ に転送されません。
- プロキシ ポートがデフォルトの Web ポートと異なる場合は、AnyConnect Web セキュリティ プロファイルの kdf リスニング ポートの一覧にプロキシ ポートを追加する必要があります。

Web スキャニング サービスでのエンドポイント トラフィックの除外または包含

Cisco Cloud Web Security スキャニングで特定のネットワーク トラフィックを除外または包含するには、Web セキュリティ プロファイル エディタを使用して該当トラフィックに対する例外を設定します。次の複数のカテゴリの例外を設定できます。

- [ホスト例外（Host Exceptions）] または [ホスト包含（Host Inclusions）] : [ホスト例外（Host Exceptions）] が設定されている場合、入力する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）はバイパスされます。[ホスト包含（Host Inclusions）] が設定されている場合、入力する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）は Web セキュリティ プロキシに転送されますが、その他のトラフィックはすべてバイパスされます。

（注） AnyConnect は、[ホスト例外（Host Exceptions）] にリストされているトラフィックも代行受信できます。

- [プロキシ例外（Proxy Exceptions）] : ここにリストされている内部プロキシ サーバは、スキャンから除外されます。
-
- [静的な例外（Static Exceptions）] : ここにリストされている IP アドレスまたはホスト名は、スキャンおよび AnyConnect から除外されます。

ISE サーバ要件

ISE サーバは、静的な例外リストに常に記載されている必要があります。このリストは、Web セキュリティ クライアント プロファイルの [例外（Exceptions）] ペインに設定されています。さらに、ISE ポスチャ クライアントが ISE サーバに到達できるように、Web セキュリティ モ

ジュールはISEポスチャ プローブをバイパスする必要があります。ISEポスチャ プロファイルは、ISE サーバを検出するために次の順序でネットワーク プローブを送信します。

1. デフォルト ゲートウェイ
2. Discovery host
3. enroll.cisco.com
4. 以前に接続した ISE サーバ

ホスト例外の除外と包含

始める前に

- トップレベル ドメインの両側にワイルドカードを使用しないでください（たとえば *.cisco.*）。これによりフィッシング サイトが含まれることがあるためです。
- デフォルトのホスト例外エントリを削除または変更しないでください。

[ホスト例外（Host Exceptions）] と [ホスト包含（Host Inclusions）] のいずれかを設定することを選択できます。[ホスト例外（Host Exceptions）] を選択した場合、指定された IP アドレスは Cisco クラウド Web セキュリティ プロキシによりバイパスされます。[ホスト包含（Host Inclusions）] を選択した場合、指定された IP アドレスは Cisco クラウド Web セキュリティ プロキシに転送され、その他のトラフィックはすべてバイパスされます。AnyConnect は除外されたホスト例外からのインターネット トラフィックを引き続き代行受信する場合があることに注意してください。Web Security と AnyConnect の両方からのトラフィックを除外するには、静的な例外を設定します。

手順

ステップ 1 [ホスト例外（Host Exceptions）] または [ホスト包含（Host Inclusions）] を選択します。

ステップ 2 ステップ 1 の選択に応じてバイパスまたは転送する IP アドレス（パブリックまたはプライベート、ホスト名、またはサブネット）を追加します。

ステップ 3 次の構文を使用してサブネットと IP アドレスを入力します。

構文	例
個々の IPv4 および IPv6 アドレス	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
Classless Inter-Domain Routing（CIDR）表記	10.0.0.0/8 2001:DB8::/48

完全修飾ドメイン名	windowsupdate.microsoft.com ipv6.google.com （注） 部分的なドメインはサポートされません。たとえば、example.com はサポートされません。
完全修飾ドメイン名または IP アドレスのワイルドカード	127.0.0.* *.cisco.com

（注） ホスト例外リストでドメイン名を使用するように Web セキュリティが設定されている場合、ユーザがホスト HTTP ヘッダー エントリをスプーフィングして Web セキュリティ プロキシをバイパスできます。例外リストでホスト名の代わりに IP アドレスを使用すると、このリスクを緩和できます。

Web セキュリティとローミング セキュリティの互換性に必須のホスト例外

Umbrella ローミング セキュリティ モジュールと Web セキュリティ モジュールを一緒に展開している場合は、ホスト例外として *.opendns.com を設定する必要があります。この設定に失敗すると、Umbrella ローミング セキュリティ DNS 保護は完全にバイパスされます。

また、Web セキュリティと Umbrella ローミング セキュリティ モジュールの互換性に必須の静的な例外 （11 ページ）に記載されている静的な例外の除外を設定する必要があります。

プロキシ例外の除外

[プロキシ例外（Proxy Exceptions）] 領域には、認証された内部プロキシの IP アドレスを入力します（例：`172.31.255.255`）。

このフィールドに IPv4 および IPv6 アドレスを指定できますが、ポート番号を一緒に指定することはできません。CIDR 表記を使用して IP アドレスを指定できません。

IP アドレスを指定すると、Cisco Cloud Web Security が、これらのサーバ宛の Web データを代行受信して SSL を使用してデータをトンネルしないようにします。プロキシ サーバは、サービスを中断させることなく実行できます。プロキシ サーバを追加しなかった場合は、Cisco Cloud Web Security トラフィックが SSL トンネルのように見えます。

プロキシサーバ経由のブラウザのトラフィックを除外する場合は、それらのホスト名をホスト例外でリストし、転送されないようにする必要があります。プロキシを通過するトラフィックの静的な例外を設定できないだけでなく、プロキシ例外リストにリストすることもできません。

このリストに存在しないプロキシの場合、Web セキュリティは SSL を使用してプロキシにトンネルしようとします。したがって、インターネットアクセスのためにプロキシをネットワークから除外する必要がある別の企業サイトにユーザが存在する場合、Cisco Cloud Web Security ではオープンなインターネット接続を利用しているかのような同じレベルのサポートが提供されます。

静的な例外の除外

Cisco Cloud Web Security をバイパスするトラフィックを決定し、Classless Inter-Domain Routing（CIDR）表記での個々の IP アドレスまたは IP アドレス範囲のリストを追加します。リストには、VPN ゲートウェイの入力 IP アドレスを含めます。AnyConnect リリース 4.3.02039 以降を使用すると、スキャンから除外するホスト名を追加できます。Web セキュリティは、インスペクションのためにクラウド Web セキュリティ プロキシに HTTP/HTTPS トラフィックを転送しません。

同じ IP アドレスの複数のホスト名があるが、ホスト名の 1 つが静的な例外リストに設定されている場合は、Web セキュリティはトラフィックを除外します。

http://www.ietf.org/rfc/rfc1918.txt に記載されたプライベート IP アドレスは、デフォルトで静的な例外リストに含まれています。

（注） 静的な例外リストのいずれかの範囲に含まれる IP アドレスを持つプロキシ サーバがある場合は、ホストの例外リストにその例外を移動します。たとえば、静的な例外リストに 10.0.0.0/8 が記載されているとします。10.1.2.3 に設定されているプロキシがある場合、ホストの例外リストに 10.0.0.0/8 を移動します。そうしないと、このプロキシに送信されたトラフィックは Cloud Web Security をバイパスします。

CIDR 表記を使用して、IPv4 および IPv6 アドレスまたはアドレスの範囲を指定できます。完全修飾ドメイン名を指定したり、IP アドレスにワイルドカードを使用したりすることはできません。正しい構文の例は次のとおりです。

```
10.10.10.5
192.0.2.0/24
```

（注） SSL VPN コンセントレータの IP アドレスを静的な除外リストに追加してください。

Web セキュリティと Umbrella ローミング セキュリティ モジュールの互換性に必須の静的な例外

Umbrella ローミング セキュリティと Web セキュリティ モジュール間の相互運用性を確保するためには、AnyConnect にプロビジョニングされる Web セキュリティ プロファイルで次の例外を設定する必要があります。

- 77.67.54.0/27
- 77.67.54.32/27
- 77.67.54.64/27
- 77.67.54.96/27
- 77.67.54.128/27
- 77.67.54.160/27

- 67.215.64.0/19
- 204.194.232.0/21
- 208.67.216.0/21
- 208.69.32.0/21
- 185.60.84.0/22
- 146.112.61.0/22
- 146.112.128.0/18

また、Web セキュリティとローミング セキュリティの互換性に必須のホスト例外 （10 ページ）に記載されているホスト例外の除外を設定する必要があります。

ユーザ制御の設定および最も早いスキャニングプロキシ応答時間の計算

ユーザが、接続先の Cisco Cloud Web Security スキャニング プロキシを選択できるようにするには、次の手順を実行します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [プリファレンス（Preferences）] をクリックします。

ステップ 4 [ユーザ制御可（User Controllable）] をオンにします（これがデフォルト設定です）。[ユーザ制御可（User Controllable）] は、ユーザが AnyConnect インターフェイスで [自動タワー選択（Automatic Tower Selection）] および [応答時間によるスキャニングプロキシの順序付け（Order Scanning Proxies by Response Time）] 設定を変更できるかどうかを決定します。

ステップ 5 Web セキュリティで自動的にスキャン プロキシを選択するには、[スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択します。これを選択すると、[応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] が自動的にオンになります。

- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択すると、Web セキュリティは、応答時間が最も早いスキャニング プロキシを判別して、ユーザをそのスキャニング プロキシに自動的に接続します。
- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しなくても、まだ [応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] が選択されている場合、ユーザには、接続できるスキャニング プロキシのリストが、応答時間が早い順に表示されます。
- [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を選択しない場合でも、ユーザが AnyConnect ユーザ インターフェイスでこの機能を有効にできますが、いったん有効にすると、再度無効に切り替えることができません。

（注） [スキャンプロキシの自動選択（Automatic Scanning Proxy Selection）] を有効にすると、一時的な通信の中断と障害が原因で、アクティブなスキャニング プロキシの選択が自動的に変更される可能性があります。スキャニング プロキシの変更は不適切な場合があり、異なる言語を使用する異なる国のスキャニング プロキシから検索結果が返されるなど、予期しない動作を引き起こすことがあります。

ステップ 6 [応答時間によるスキャニング プロキシの順序付け（Order Scanning Proxies by Response Time）] をオンにした場合は、応答時間が最も早いスキャニング プロキシを計算するための次の設定を行います。

- [テスト間隔の有効化（Enable Test Interval）]：各パフォーマンス テストの実行間の時間（時間および分単位。デフォルトは 2 分間です）。[テスト間隔の有効化（Enable Test Interval）] チェックボックスをオフにすることで、テスト間隔をオフにして、テストが実行されないようにできます。
- [テストの非アクティブ タイムアウト（Test Inactivity Timeout）]：Web セキュリティが、ユーザ非アクティブのために応答時間テストを一時停止するまでの時間（分単位）。Web セキュリティは、スキャニング プロキシで接続試行が行われるとすぐにテストを再開します。この設定は、カスタマーサポートから指示された場合以外は変更しないでください。

（注） [応答時間によるスキャニング プロキシの順序付け（Ordering Scanning Proxies by Response Time）] テストは、次の例外を除き、テスト間隔に基づいて実行し続けます。

- Secure Trusted Network Detection が有効で、マシンが社内 LAN 上にあることが検出された。
- Web セキュリティのライセンス キーがないか、無効である。
- ユーザが、設定済みの時間非アクティブで、その結果 [テストの非アクティブ タイムアウト（Test Inactivity Timeout）] しきい値に達した。

ステップ 7 エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出する [セキュアな信頼ネットワーク検出（Secure Trusted Network Detection）] をクリックし、有効化します。有効になっている場合、社内 LAN から発信される

すべてのネットワーク トラフィックは、Cisco Cloud Web Security スキャニング プロキシをバイパスします。

ステップ 8 [https] フィールドに各信頼サーバの URL を入力し、[追加（Add）] をクリックします。URL にはポート アドレスを含めることができます。プロファイル エディタは、信頼サーバへの接続を試みます。接続できなくても、サーバ証明書の SHA-256 ハッシュがわかっている場合は、それを [証明書ハッシュ（Certificate hash）] ボックスに入力し、[設定（Set）] をクリックします。

ステップ 9 Web セキュリティ クライアント プロファイルを保存します。

次のタスク

詳細については、『*ScanCenter Administrator Guide, Release 5.2*』を参照してください。

Secure Trusted Network Detection の使用

Secure Trusted Network Detection 機能は、エンドポイントが社内 LAN 上に物理的に存在するタイミング、または VPN 接続を使用して存在するタイミングを検出します。Secure Trusted Network Detection 機能が有効になっている場合、社内 LAN からのネットワーク トラフィックはすべて、送信元の Cisco Cloud Web Security スキャニング プロキシをバイパスします。そのトラフィックのセキュリティは、Cisco Cloud Web Security ではなく、社内 LAN に存在するデバイスにより別の方法で管理されます。

Secure Trusted Network Detection では、既知の URL（アドレス、IP、または FQDN）にあるサーバ上の SSL 証明書の SHA-256 ハッシュ（サムプリント）を使用してクライアントが社内ネットワークに接続されていることを確認します。証明書によって使用される暗号化アルゴリズムは問いませんが、SHA-256 ハッシュのみを使用できます。

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [例外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。

複数のサーバ：複数のサーバを定義すると、クライアントが最初のサーバに対して 2 回連続試行しても接続できない場合に、2 番目のサーバに対して試行します。クライアントは、リスト内のすべてのサーバに対して試行した後、5 分間待ってから、最初のサーバに再接続を試みます。

（注） 内部ネットワークの外から操作する場合は、Secure Trusted Network Detection が DNS 要求を行い、プロビジョニングした HTTPS サーバに接続を試みます。シスコでは、内部ネットワークの外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアス設定の使用をお勧めします。

始める前に

- プロキシ例外の除外

- データ損失の防止（DLP）アプライアンスなどの一部のサードパーティ製ソリューションでは、Webセキュリティの影響を受けないトラフィックが必要になるため、Secure Trusted Network Detection を設定することが必要となります。
- プロファイルを編集するときは、SSL 証明書がホストされるサーバへの直接接続があることを確認します。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[プリファレンス（Preferences）] をクリックします。

ステップ 4 [Trusted Network Detection の有効化（Enable Trusted Network Detection）] を選択します。

ステップ 5 [https] フィールドに各信頼サーバの URL を入力し、[追加（Add）] をクリックします。URL にはポート アドレスを含めることができます。プロファイル エディタは、信頼サーバへの接続を試みます。接続できなくても、サーバ証明書の SHA-256 ハッシュがわかっている場合は、それを [証明書ハッシュ（Certificate hash）] ボックスに入力し、[設定（Set）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

ステップ 6 Web セキュリティ クライアント プロファイルを保存します。

Secure Trusted Network Detection の不使用

ネットワークにプロキシが存在する（Cisco Cloud Web Security コネクタなど）状態で、Secure Trusted Network Detection を使用しない場合は、プロファイル エディタの [例外（Exceptions）] パネルで、プロキシ例外のリストに各プロキシを追加する必要があります。

認証の設定および Cisco Cloud Web Security プロキシへのグループ メンバーシップの送信

始める前に

Windows を使用したフィルタの無効化と有効化 （26 ページ）

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [認証（Authentication）] をクリックします。

ステップ 4 [プロキシ認証ライセンス キー（Proxy Authentication License Key）] フィールドに、Cisco ScanCenter で作成した企業キー、グループ キー、またはユーザ キーに対応するライセンス キーを入力します。これらの企業ドメインに基づいてユーザを認証するには、作成した企業キーを入力します。Cisco ScanCenter または Active Directory グループに基づいてユーザを認証するには、作成したグループ キーを入力します。デフォルトでは、このタグは空です。空のままにした場合、Web セキュリティはパススルー モードで動作します。

ステップ 5 [サービス パスワード（Service Password）] に入力します。Web セキュリティのデフォルト パスワードは websecurity です。プロファイルのカスタマイズ時にこのパスワードを変更してください。パスワードには英数字（a ～ z、A ～ Z、0 ～ 9）のみを使用する必要があります。次のような特殊文字は、Windows コマンド シェルによって制御文字と間違われる可能性があるか、XML で特殊な意味を持つことがあります。

```
~ @ # $ % * - _ + = { } [ ] : , . ? /
```

このパスワードを使用して、管理者の権限を持っているユーザは、Web セキュリティ サービスを停止できます。管理者権限を持つユーザまたは持たないユーザは、このパスワードなしで Web セキュリティ サービスを開始できます。

ステップ 6 すべての HTTP 要求とともに企業ドメイン情報および Cisco Cloud Web Security または Active Directory グループ情報をスキャニング プロキシ サーバに送信します。スキャニング プロキシは、ユーザのドメインおよびグループ メンバーシップについて認識している内容に基づいてトラフィック フィルタリング ルールを適用します。

（注） ユーザのカスタム ユーザ名およびカスタム グループ情報をスキャニング サーバ プロキシに送信するには、このステップをスキップし、ステップ 7 に進みます。Active Directory を使用しない企業の場合は、ステップ 7 もスキップしてください。

a) [企業ドメインの有効化（Enable Enterprise Domains）] をクリックします。リストから [すべてのドメイン（All Domains）] をクリックします。[すべてのドメイン（All Domains）] オプションが選択され、マシンがドメイン内にある場合、ユーザが属するドメインが照合され、ユーザ名とグループ メンバーシップ情報が Cisco Cloud Web Security スキャニング プロキシに送信されます。このオプションは、社内に複数のドメインがある場合に役立ちます。

b) または、[個々のドメインの指定（Specify Individual Domains）] をクリックします。

NetBIOS 形式で各ドメイン名を入力し、[追加（Add）] をクリックします。たとえば、`example.cisco.com` の NetBIOS 形式は cisco です。DNS 形式を使用したドメイン名（abc.def.com）を入力しないでください。

[企業ドメイン名（Enterprise Domain name）] フィールドにドメイン名を指定すると、Cisco Cloud Web Security は、現在ログインしている Active Directory ユーザを識別し、そのユーザの Active Directory グループを列挙し、その情報をすべての要求とともにスキャニング プロキシに送信します。

c) [使用（Use）] リストで、[グループ包含リスト（Group Include List）] または [グループ除外リスト（Group Exclude List）] をクリックし、Cisco Cloud Web Security スキャニング プロキシに対する HTTP 要求でグループ情報を含めるか除外します。値には、照合する文字列の任意の部分文字列を指定できます。

[グループ包含リスト（Group Include List）]。[グループ包含リスト（Group Include List）] を選択した後、Cisco Cloud Web Security グループ名または Active Directory グループ名を [グループ包含リスト（Group Include List）] に追加します。これらのグループ名は、HTTP 要求とともに Cisco Cloud Web Security スキャニング プロキシ サーバに送信されます。要求が、指定された企業ドメイン内のユーザから出された場合、HTTP 要求は、ユーザのグループ メンバーシップに従ってフィルタリングされます。ユーザにグループ メンバーシップがない場合、HTTP 要求は、デフォルトのフィルタリング ルール セットを使用してフィルタリングされます。

[グループ除外リスト（Group Exclude List）]。[グループ除外リスト（Group Exclude List）] に、Cisco Cloud Web Security グループ名または Active Directory グループ名を追加します。これらのグループ名は、HTTP 要求とともに Cisco Cloud Web Security スキャニング プロキシ サーバに送信されません。ユーザが、[グループ除外リスト（Group Exclude List）] のいずれかのグループに属している場合、そのグループ名はスキャニング プロキシ サーバに送信されず、ユーザの HTTP 要求は、その他のグループ メンバーシップ、または最低でも Active Directory または Cisco Cloud Web Security グループ所属を持たないユーザに対して定義されたデフォルトのフィルタリング ルール セットのいずれかによってフィルタリングされます。

ステップ 7 スキャニング プロキシ サーバのカスタム名を送信するには、[ドメインに参加していないマシンのカスタム照合およびレポート（Custom matching and reporting for machines not joined to domains）] をクリックします。

a) コンピュータの名前を使用するには、リストの [コンピュータ名（Computer Name）] をクリックします。または、ローカル ユーザ名を使用するには、[ローカル ユーザ（Local User）] をクリックします。または、カスタム ユーザ名を入力するには、[カスタム名（Custom Name）] をクリックします。これは、任意の文字列で定義できます。文字列を入力しない場合、代わりにコンピュータの IP アドレスが、スキャニング プロキシ サーバに送信されます。このユーザ名または IP アドレスは、カスタム ユーザから HTTP トラフィックを識別する Cisco ScanCenter レポートで使用されます。

b) [認証グループ（Authentication Group）] フィールドに、最大 256 文字の英数字のカスタム グループ名を入力し、[追加（Add）] をクリックします。

HTTP 要求がスキャニング プロキシ サーバに送信されると、カスタム グループ名が送信された場合に、スキャニング プロキシ サーバに対応するグループ名があれば、HTTP トラフィックは、カスタム グループ名に関連付けられたルールによってフィルタリングされます。スキャニング プロキシ サーバで定義された対応するカスタム グループがない場合、HTTP 要求はデフォルト ルールによってフィルタリングされます。

カスタム ユーザ名のみを設定し、カスタム グループを設定していない場合、HTTP 要求は、スキャニング プロキシ サーバのデフォルト ルールによってフィルタリングされます。

ステップ 8 Web セキュリティ クライアント プロファイルを保存します。

Web セキュリティの詳細設定

Web セキュリティ クライアント プロファイルの [詳細（Advanced）] パネルには、シスコ カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ついくつかの設定が表示されます。このパネルの設定は、カスタマー サポートから指示された場合以外は変更しないでください。

プロファイル エディタの [詳細（Advanced）] パネルから、次のタスクを実行します。

KDF リスニング ポートの設定

Kernel Driver Framework（KDF）は、トラフィック リスニング ポートの 1 つを宛先ポートとして使用する接続をすべて代行受信して、トラフィックを KDF リスニング ポートに転送します。Web スキャニング サービスは、KDF リスニング ポートに転送されるトラフィックをすべて分析します。

始める前に

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 4 [KDF リスニング ポート（KDF Listen Port）] フィールドに KDF リスニング ポートを指定します。

ステップ 5 Web セキュリティ クライアント プロファイルを保存します。

ポートが着信接続を受信する方法の設定

サービス通信ポートは、Web スキャニング サービスが、AnyConnect GUI コンポーネントおよびその他のユーティリティ コンポーネントからの着信接続を受信するポートです。

始める前に

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [編集（Edit）] をクリックします。[Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 3 [サービス通信ポート（Service Communication Port）] フィールドを編集します。

ステップ 4 Web セキュリティ クライアント プロファイルを保存します。

（注） デフォルト値の 5300 からポートを変更した場合は、Web セキュリティ サービスと AnyConnect GUI コンポーネントをリスタートする必要があります。

タイムアウトと再試行が発生するタイミングの設定

接続タイムアウト設定によって、Web セキュリティがスキャニング プロキシを使用せずにインターネットにアクセスしようとするまでのタイムアウトを設定できます。空白のままにすると、デフォルト値の 4 秒が使用されます。この設定により、ユーザは再試行までのタイムアウトを待つことなく、有料ネットワーク サービスに迅速にアクセスできます。

手順

ステップ 1 次のいずれかの方法で、Web セキュリティ プロファイル エディタを起動します。

- ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** を選択します。
- Windows のスタンドアロン モードで、**[スタート（Start）] > [すべてのプログラム] > [Cisco] > [Cisco AnyConnect プロファイル エディタ（Cisco AnyConnect Profile Editor）] > [Web セキュリティ プロファイル エディタ（Web Security Profile Editor）]** を選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを開きます。

ステップ 3 [Web セキュリティ（Web Security）] ツリー ペインで、[詳細（Advanced）] をクリックします。

ステップ 4 [接続タイムアウト（Connection Timeout）] フィールドを変更します。

ステップ 5 Web セキュリティ クライアント プロファイルを保存します。

DNS ルックアップ

プロファイル エディタの [詳細（Advanced）] パネルには、ドメイン ネーム サーバ ルックアップを管理するためのフィールドがいくつか含まれています。これらは、DNS ルックアップに最適な値で設定されています。

ガイドライン

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

デバッグの設定

[デバッグ レベル（Debug Level）] は設定可能なフィールドです。

ガイドライン

この設定は、カスタマー サポートから指示された場合以外は変更しないでください。

トラフィックのブロックと許可

Cisco Cloud Web Security プロキシ サーバへの接続が確立できない場合、トラフィックをブロックするように [接続障害ポリシー（Connection Failure Policy）] リストで [フェール クローズ（Fail Close）] を選択します。または、[フェール オープン（Fail Open）] を選択し、トラフィックを許可します。

Cisco Cloud Web Security プロキシ サーバへの接続が確立できないけれども、Wi-Fi ホット スポットなどのキャプティブ ポータルが検出された場合に、トラフィックを許可するには、[キャプティブ ポータルが検出された場合（When a captive portal is detected）] リストで [フェール オープン（Fail Open）] を選択します。または、[フェール クローズ（Fail Close）] を選択し、トラフィックをブロックします。

（注） キャプティブ ポータルのアドレスを含めるようにホスト、プロキシ、または静的な例外が設定されている場合、[フェール クローズ（Fail Close）] はトラフィックをブロックしません。

他のカスタマイズ可能な Web セキュリティ オプション

エクスポート オプション

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

難解化 Web セキュリティ クライアント プロファイルを ASA からエクスポートして、エンドポイント デバイスに配布します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** の順に選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3 ファイルを保存するローカル フォルダを参照します。[ローカル パス（Local Path）] フィールドのファイル名を編集すると、その新しいファイル名で Web セキュリティ クライアント プロファイルが保存されます。

ステップ 4 [エクスポート（Export）] をクリックします。

ASDM は、Web セキュリティ クライアント プロファイルのプレーン テキスト バージョンである `filename.wsp` をエクスポートします。

DART バンドルのプレーン テキストの Web セキュリティ クライアント プロファイル ファイルのエクスポート

Diagnostic AnyConnect Reporting Tool（DART）バンドルをシスコのカスタマー サービスに送信する必要がある場合、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイル ファイル（`filename.wsp` または `filename.xml`）を DART バンドルとともに送信する必要があります。シスコ カスタマー サービスは難読化されたバージョンを読み取ることはできません。

プロファイル エディタのスタンドアロン バージョンは、Web セキュリティ プロファイル ファイルの 2 つのバージョンを作成します。1 つはファイル名が `filename.wso` の難解化ファイル、もう 1 つはファイル名が `filename.xml` のプレーン テキスト ファイルです。

DART バンドルをシスコのカスタマー サービスに送信する前に、プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルを DART バンドルに追加します。

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルの編集および ASDM からのインポート

プレーン テキストの Web セキュリティ クライアント プロファイル ファイルをエクスポートした場合は、ローカル コンピュータで、AnyConnect Web セキュリティ プロファイル エディタでサポートされていない編集が可能ないずれかのプレーン テキストまたは XML エディタを使用して編集します。プレーン テキスト バージョンの Web セキュリティ クライアント プロファイルは、カスタマーサポートから指示された場合以外は変更しないでください。エディタをインポートするには、次の手順を実行します。

始める前に

ファイルをインポートすると、選択した Web セキュリティ クライアント プロファイルの内容は上書きされます。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]** の順に選択します。

ステップ 2 編集する Web セキュリティ クライアント プロファイルを選択して [エクスポート（Export）] をクリックします。

ステップ 3 `filename.wsp` を変更した後で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページに戻って、編集したファイルのプロファイル名を選択します。

ステップ 4 [インポート（Import）] をクリックします。

ステップ 5 編集したバージョンの Web セキュリティ クライアント プロファイルを参照して、[インポート（Import）] をクリックします。

難解化 Web セキュリティ クライアント プロファイル ファイルのエクスポート

手順

ステップ 1 ASDM を開き、**[ツール（Tools）] > [ファイル管理（File Management）]** を選択します。

ステップ 2 [ファイル管理（File Management）] 画面で、**[ファイル転送（File Transfer）] > [ローカル PC とフラッシュ間（Between Local PC and Flash）]** をクリックして、[ファイル転送（File Transfer）] ダイアログを使用して難解化 `filename.wso` クライアント プロファイル ファイルをローカル コンピュータに転送します。

Web セキュリティのためのスプリット トンネル除外の設定

ユーザが VPN セッションを確立した場合は、すべてのネットワーク トラフィックが VPN トンネル経由で送信されます。ただし、AnyConnect ユーザが Web セキュリティを使用している場合、エンドポイントで発信された HTTP トラフィックはトンネルから除外され、クラウド Web セキュリティ スキャニング プロキシに直接送信される必要があります。

クラウド Web セキュリティ スキャニング プロキシ用のトラフィックのスプリット トンネル除外を設定するには、グループ ポリシーで [Web セキュリティのためのスプリット除外の設定（Set up split exclusion for Web Security）] ボタンを使用します。

始める前に

- AnyConnect クライアントで使用するように Web セキュリティを設定します。
- グループ ポリシーを作成して、Web セキュリティが設定された AnyConnect クライアントの接続プロファイルを割り当てます。

Secure Trusted Network Detection 機能を使用する場合に、Web セキュリティと VPN が同時にアクティブになるようにするには、HTTPS サーバが VPN トンネル経由で到達可能にならないようにネットワークを設定します。この方法では、ユーザが社内 LAN 上にいるときに限り、Web セキュリティ機能はバイパス モードになります。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 **[詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）]** を選択します。

ステップ 4 [Web セキュリティのためのスプリット除外の設定（Set up split exclusion for Web Security）] をクリックします。

ステップ 5 Web セキュリティのスプリット除外に使用される新しいアクセス リストを入力するか、既存のアクセス リストを選択します。ASDM は、ネットワーク リストで使用するアクセス リストを設定します。

ステップ 6 新しいリストの場合は [アクセス リストの作成（Create Access List）] をクリックし、既存のリストの場合は [アクセス リストの更新（Update Access List）] をクリックします。

ステップ 7 [OK] をクリックします。

次のタスク

追加スキャニング プロキシを追加した場合は、この手順で作成した統合アクセス リストを新しい情報で更新します。

Cisco Cloud Web Security ホステッド プロファイルの使用

AnyConnect リリース 3.0.4 から、Web セキュリティ ホステッド クライアント プロファイルの Cisco ScanCenter ホステッド コンフィギュレーションにより、Web セキュリティ クライアントに新しい設定を提供できます。Web セキュリティを備えたデバイスは、クラウドから新しい Web セキュリティ ホステッド クライアント プロファイルをダウンロードできます（ホステッド コンフィギュレーション ファイルは Cisco ScanCenter サーバに格納されています）。

AnyConnect クライアントは、リソース サービスから AnyConnect バイナリにハードコード化されているホスト名を使用してコンフィギュレーション ファイルをダウンロードする必要があります。要求は hostedconfig.scansafe.net/（IP：46.155.41.2）に対して行われ、通信は TCP ポート 443 で暗号化されます。

ホスト設定で、AnyConnect Web セキュリティに TCP ポート 443（およびプレーン モードで展開している場合はポート 8080）からの CWS タワー/プロキシの入力 IP へのアクセスを許可します。AnyConnect Web セキュリティのタワー/プロキシの完全なリストは、『Cisco ScanCenter Administration Guide』の「**Prepare**」セクションに記載されています。クライアントは TCP ポート 80 で 80.254.145.118 にアクセスできる必要があります。このアクセスにより、プロキシ タワーのリストを取得し、最新に保ちます。Web セキュリティ モジュールは TCP ポート 80 で Verisign に接続するように設定する必要があります。この範囲では、クライアントは証明書失効を Tj.symbcb.com、T1.symcb.com、および T2.symcb.com でチェックします。

Web セキュリティ プロファイル エディタを使用してクライアント プロファイルを作成してから、クリア テキスト XML ファイルを Cisco ScanCenter サーバにアップロードします。この XML ファイルには、同じ会社、グループ、またはユーザ ライセンス キーが Cisco Cloud Web Security で定義されホストされたホスト設定と関連付けられている、有効なライセンス キーを含める必要があります。クライアントは、ホステッド コンフィギュレーション サーバに適用されてから 8 時間以内に、新しいコンフィギュレーション ファイルを取得します。

ホステッド コンフィギュレーション機能では、ホステッド コンフィギュレーション（Cisco ScanCenter）サーバから新しいクライアント プロファイル ファイルを取得する際にライセンス キーが使用されます。新しいクライアント プロファイル ファイルがサーバ上に置かれたら、Webセキュリティを実装したデバイスは自動的にサーバをポーリングし、新しいクライアント プロファイルをダウンロードします。これには、既存の Web セキュリティ クライアント プロファイルにあるライセンスがホステッド サーバ上のクライアント プロファイルに関連付けられたライセンスと同じであることが条件となります。新しいクライアントプロファイルをダウンロードした場合、新しいクライアント プロファイル ファイルを使用可能にするまで Web セキュリティは同じファイルを再度ダウンロードしません。

ライセンス キーの詳細については、『*Cisco ScanCenter Administration Guide, Release 5.2*』を参照してください。

始める前に

- Web セキュリティ クライアント デバイスを、Cisco Cloud Web Security ライセンス キーを含む有効なクライアント プロファイルを使用してインストールします。
- Web セキュリティ エージェント サービスのリスタート オプションは、サービスを再開するために必要な権限を持つユーザのみが使用可能です。
- ACWS エージェントを実行するクライアント コンピュータは、信頼されたルート証明機関ストアの Thawte プライマリ ルート CA および Thawte SSL CA - G2 が必要です。

手順

ステップ 1 Web セキュリティ プロファイル エディタを使用して、Web セキュリティ デバイス用の新しいクライアントプロファイルを作成します。このクライアントプロファイルは、Cisco Cloud Web Security ライセンス キーを含んでいる必要があります。

ステップ 2 クライアント プロファイル ファイルをクリア テキストの XML ファイルとして保存します。このファイルを Cisco ScanCenter サーバにアップロードします。このファイルをアップロードしたら、新しいクライアント プロファイルを Web セキュリティ クライアントに対して使用可能にします。

ステップ 3 新しいクライアント プロファイルをアップロードし、会社の Cisco ScanCenter を介して適用します。ただし、ホステッドコンフィギュレーション機能が会社で有効になっている必要があります。ホステッド クライアント プロファイルはライセンスに関連付けられています。異なるライセンス（たとえば、異なるグループのライセンス キー）を使用している場合、各ライセンスに独自のクライアントプロファイルを関連付けることができます。ユーザに設定されているライセンスに応じて、異なるユーザに異なるクライアントプロファイルを適用できます。ライセンスごとにさまざまな設定を格納して、クライアントがダウンロードするデフォルト クライアント プロファイルを設定します。その後、クライアントは、Cisco ScanCenter のホステッド コンフィギュレーションエリアに格納されている他のリビジョンの設定の 1 つをデフォルトとして選択することで、そのクライアントプロファイルに切り替えることができます。1 つのラ

イセンスは、1つのクライアントプロファイルのみに関連付けられます。したがって、複数のリビジョンがライセンスに関連付けられている場合、デフォルトにできるのは1つだけです。

Cisco AnyConnect Web セキュリティ エージェントの無効化および有効化

次の手順を実行することで、Web トラフィックを代行受信する Cisco AnyConnect Web セキュリティ エージェントの機能を無効化および有効化できます。

Windows を使用したフィルタの無効化と有効化

手順

ステップ 1 コマンド プロンプト ウィンドウを開きます。

ステップ 2 **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** フォルダに移動します。

ステップ 3 フィルタリングを有効または無効にします。

- フィルタリングを有効にするには、**acwebsecagent.exe -enablesvc** と入力します。
- フィルタリングを無効にするには、**acwebsecagent.exe -disablesvc -servicepassword** と入力します。

Mac OS X を使用したフィルタの無効化と有効化

サービス パスワードは、Web セキュリティ プロファイル エディタの [認証（Authentication）] パネルで設定します。

手順

ステップ 1 ターミナル アプリケーションを起動します。

ステップ 2 /opt/cisco/anyconnect/bin フォルダに移動します。

ステップ 3 フィルタリングを有効または無効にします。

- フィルタリングをオンにするには、**./acwebsecagent -enablesvc** と入力します。
- フィルタリングを無効にするには、**./acwebsecagent -disablesvc -servicepassword** と入力します。

Web セキュリティ ロギング

Windows

すべての Web セキュリティ メッセージは、Windows イベント ビューアの `Event Viewer (Local)\Cisco AnyConect Web Security Module` フォルダに記録されます。Web セキュリティがイベント ビューアに記録するイベントは、Cisco Technical Assistance Center のエンジニアが分析します。

Mac OS X

Web セキュリティ メッセージは、syslog またはコンソールから表示します。