# 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 （11 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 （13 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 （18 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** ScanSafe 汎用オプション コンフィギュレーション モードを開始します。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。

**scansafe general-options**

例：

```
hostname(config)# scansafe general-options
```

**ステップ 2** プライマリおよびセカンダリ クラウド Web セキュリティ プロキシ サーバを設定します。

**server primary** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

**server backup** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

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。それらの IP アドレス（**ip**）または完全修飾ドメイン名（**fqdn**）を上記のコマンドに入力します。

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。

例：

```
hostname(cfg-scansafe)# server primary ip 192.168.43.10
hostname(cfg-scansafe)# server backup fqdn server.example.com
```

**ステップ 3** （任意）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設定します。

**retry-count** *value*

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。

例：

```
hostname(cfg-scansafe)# retry-count 2
```

**ステップ 4** （任意）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。

a) アプリケーション健全性チェックを有効にします。

**health-check application** [**url** *url_string*]

Cisco クラウド Web セキュリティによって指示された場合にのみ、URL を指定します。URL は、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ます。デフォルトの URL は http://gs.scansafe.net/goldStandard?type=text&size=10 です。その URL が必要とされるものでなくなった場合は、Cisco から提供された新しい URL を指定します。

例：

```
hostname(cfg-scansafe)# health-check application
```

b) ヘルス チェックのポーリング タイムアウトを設定します。

**health-check application timeout** *seconds*

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。

例：

```
hostname(cfg-scansafe)# health-check application timeout 20
```

**ステップ 5** 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を設定します。

**license** *hex_key*

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。

例：

```
hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3
```

**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。

**scansafe** [**license** *hex_key*]

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。

例：

```
hostname(config)# changeto context one
hostname/one(config)# scansafe
```

### 例

次に、プライマリ サーバとバックアップ サーバを設定する例を示します。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 health-check application
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

次に、デフォルトのライセンスを使用してコンテキスト 1 でクラウド Web セキュリティをイネーブルにし、ライセンス キーの上書きを使用してコンテキスト 2 でクラウド Web セキュリティをイネーブルにする設定の例を示します。

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

# 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** クラス マップを作成します。**class-map type inspect scansafe** [**match-all** | **match-any**] *class_map_name*

*class_map_name* には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。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 キーワードは、トラフィックが少なくとも 1 つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

例：

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
```

**ステップ 2** ホワイトリストに記載されたユーザおよびグループを指定します。

**match** [**not**] {[**user** *username*] [**group** *groupname*]}

**match** キーワードは、ホワイトリストに記載するユーザまたはグループ、あるいはその両方を指定します。

**match not** キーワードはユーザまたはグループがクラウド Web セキュリティを使用してフィルタリングされる必要があることを指定します。たとえば、グループ「cisco」をホワイトリストに記載し、そのグループのメンバーであるユーザ「johncrichton」および「aerynsun」からのトラフィックをスキャンする場合、これらのユーザに **match not** を指定できます。このコマンドを繰り返して、必要な数のユーザおよびグループを追加します。

### 例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザおよびグループをホワイトリストに記載する例を示します。

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
```

```
hostname(config-pmap-c)# whitelist
```

# 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** ScanSafe インスペクション ポリシー マップを作成します。HTTP と HTTPS に対して別々のマップを定義する必要があります。

a) ScanSafe インスペクション ポリシー マップを作成します。**policy-map type inspect scansafe** *policy_map_name*

*policy_map_name* には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

b) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

c) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- {**ip** | **https**}：このマップのサービス タイプ。マップごとに 1 つのサービス タイプしか指定できないため、HTTP と HTTPS に対して別々のマップが必要です。

- **default** {[**user** *username*] [**group** *groupname*]}：（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。

d) （任意）ホワイトリストを定義した場合、クラスを識別し、**whitelist** コマンドを使用してホワイトリストとしてマークします。

```
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

e) このプロセスを繰り返して、他のプロトコル、HTTP、または HTTPS のインスペクション ポリシー マップを作成します。

**ステップ 2** 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のクラスを定義します。

ACL マッチングは、クラスを定義する最も柔軟な方法です。ただし、すべての HTTP/HTTPS トラフィックを送信する場合は、クラス内のポート一致を使用できます（**match port tcp 80** および **match port tcp 443**）。次の手順では、ACL 一致について説明します。

a) ACL を作成して（**access-list extended** コマンド）、クラウド Web セキュリティに送信するトラフィックを識別します。HTTP と HTTPS のトラフィックに対して別々の ACL を作成する必要があります。クラウド Web セキュリティは HTTP/HTTPS トラフィックでのみ機能するため、ACL に定義されたその他のトラフィックは無視されます。

**許可** ACE は、クラウド Web セキュリティに一致したトラフィックを送信します。**拒否** ACE は、クラウド Web セキュリティに送信されないように、トラフィックをサービス ポリシー ルールから免除します。プロトコルに **tcp** を使用して、ポート（HTTP の場合は 80、HTTPS の場合は 443）を識別します。

ACL 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を照合し、他のインターネット ネットワーク宛てのトラフィックを照合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。

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を免除するのに役立つ場合があります。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。

ポリシーに必要な数の ACL を作成します。任意の数のトラフィック クラスにリダイレクションを適用できます。

**例**：

次に、2 つのサーバへの HTTP トラフィックを免除しても、残りのトラフィックを含める例を示します。HTTPS トラフィックに重複 ACL を作成します。この場合、ポートを 443 に変更するだけです。

```
hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com

hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq
 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq
 80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
```

b) 定義した ACL ごとにトラフィック クラスを作成します。

```
hostname(config)# class-map class_name
hostname(config-cmap)# match access-list acl_name
```

**例**：

```
hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS
```

**ステップ 3** 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ポリシー マップを作成または編集します。

a) クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。**policy-map** *name*

デフォルト設定では、global_policy ポリシー マップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。各インターフェイスにポリシー マップを 1 つだけ適用するか、またはグローバルに適用できます。

**例**：

```
hostname(config)# policy-map global_policy
```

b) クラウド Web セキュリティ インスペクション用に作成したトラフィック クラス マップの 1 つを識別します。**class** *name*

**例**：

```
hostname(config-pmap)# class cws_class1
```

c) クラスの ScanSafe インスペクションを設定します。

**inspect scansafe** *scansafe_policy_map* [**fail-open** | **fail-close**]

それぞれの説明は次のとおりです。

- *scansafe_policy_map* は、ScanSafe インスペクション ポリシー マップです。クラス マップおよびポリシー マップでプロトコルを照合していることを確認します（HTTP/HTTPS）。
- **fail-open** を指定すると、クラウド Web セキュリティ サーバを使用できない場合にトラフィックが ASA を通過できます。
- **fail-close** を指定すると、クラウド Web セキュリティ サーバを使用できない場合にすべてのトラフィックがドロップされます。 **fail-close** がデフォルトです。

例：

```
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
```

（注） 別の ScanSafe インスペクション ポリシー マップを使用するためにデフォルト グローバル ポリシー（または使用中のポリシー）を編集する場合は、 **no inspect scansafe** コマンドで ScanSafe インスペクションを削除し、新しいインスペクション ポリシー マップの名前で再追加してください。

d) 他のプロトコルのクラスを追加し、インスペクションをイネーブルにします。追加クラスがある場合には、それらも追加します。

```
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
```

**ステップ 4** 既存のサービス ポリシー（たとえば、global_policy という名前のデフォルト グローバル ポリシー）を編集している場合は、以上で終了です。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

**service-policy** *policymap_name* {**global** | **interface** *interface_name*}

例：

```
hostname(config)# service-policy global_policy global
```

**global** キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

### 例

次に、2つのクラス（HTTPに1つ、HTTPSに1つ）を設定する例を示します。各ACLはwww.cisco.comとtools.cisco.com、DMZネットワーク、およびHTTPとHTTPSの両方に対するトラフィックを免除します。他のすべてのトラフィックは、複数のホワイトリストに記載されたユーザおよびグループを除き、クラウドWebセキュリティに送信されます。ポリシーは、内部インターフェイスに適用されます。

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network
eq 80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network
eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
hostname(config)# service-policy cws_policy inside
```

# 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** アクティブな ACL でまだ使用されていない ScanCenter ポリシーで使用するグループを識別します。必要に応じて、ローカル ユーザ グループ オブジェクトを作成します。

**ステップ 2** AD エージェントからグループ情報をダウンロードします。

**user-identity monitor** {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

それぞれの説明は次のとおりです。

- **user-group**：AD サーバに定義されたグループ名を指定します。
- **object-group-user**：**object-group user** コマンドを使用して作成されたローカル オブジェクトの名前。このグループには、複数のグループを含めることができます。

例：

```
hostname(config)# user-identity monitor user-group CISCO\\Engineering
```

# 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、次のコマンドを使用します。

- **show scansafe server**

  サーバが現在、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。

```
hostname# show scansafe server
hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
hostname# Backup: proxy137.scansafe.net (80.254.152.99)
```

- **show scansafe statistics**

  プロキシサーバにリダイレクトされる接続数、現在リダイレクトされている接続数、ホワイトリストに記載されている接続数など、クラウド Web セキュリティ アクティビティに関する情報を示します。

```
hostname# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

- **show service policy inspect scansafe**

  特定のポリシーによってリダイレクトまたはホワイトリストに記載された接続の数を表示します。

```
hostname(config)# show service-policy inspect scansafe
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
  Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-open"
config: 0
```

```
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

- **show conn scansafe**

  大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。

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。

## アイデンティティ ファイアウォールを使用したクラウド Web セキュリティの例

次の例は、アイデンティティ ファイアウォールのオプション設定など、シングル コンテキスト モードでの Cisco クラウド Web セキュリティの設定全体を示します。

**手順**

**ステップ 1** ASA でクラウド Web セキュリティを設定します。

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

**ステップ 2** アイデンティティ ファイアウォールの設定を行います。

グループが ScanCenter ポリシーの主な機能であるため、グループをまだ使用していない場合は、アイデンティティ ファイアウォールをイネーブルにすることを検討してください。ただし、アイデンティティ ファイアウォールはオプションです。次に、Active Directory（AD）サーバ、AD エージェントを定義してアイデンティティ ファイアウォールの設定を行い、少数のグループに対してユーザ アイデンティティ モニタをイネーブルにする例を示します。

```
aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
 server-port 389
```

```
 ldap-base-dn DC=ASASCANLAB,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
 server-type microsoft
aaa-server adagent protocol radius
 ad-agent-mode
aaa-server adagent (inside) host 192.168.116.220
 key *****
user-identity domain ASASCANLAB aaa-server AD
user-identity default-domain ASASCANLAB
user-identity action netbios-response-fail remove-user-ip
user-identity poll-import-user-group-timer hours 1
user-identity ad-agent aaa-server adagent
user-identity user-not-found enable
user-identity monitor user-group ASASCANLAB\\GROUP1
user-identity monitor user-group ASASCANLAB\\GROUPNAME
```

**ステップ 3** （任意）ホワイトリストを設定します。

クラウド Web セキュリティ フィルタリングから除外する特定のユーザまたはグループがある場合、ホワイトリストを作成できます。

```
class-map type inspect scansafe match-any whiteListCmap
 match user LOCAL\user1
```

**ステップ 4** ACL を設定します。

通過した HTTP および HTTPS パケットの数を確認できるように、個別の HTTP および HTTPS クラス マップを作成して、トラフィックを分割することを推奨します。

その後、トラブルシューティングする必要がある場合、デバッグ コマンドを実行して、各クラス マップを通過したパケットの数を識別し、HTTP または HTTPS トラフィックをさらに通過させているかを確認できます。

```
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

**ステップ 5** クラス マップを設定します。

```
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

hostname(config)# class-map cmap-https
hostname(config-cmap)# match access-list https
```

**ステップ 6** インスペクション ポリシー マップを設定します。

```
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist
```

```
hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstraffic
hostname(config-pmap-p)# https
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist
```

**ステップ 7** ポリシー マップを設定します。

次の例では、クラウド Web セキュリティ トラフィックに固有のポリシー マップを作成します。

```
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

または、デフォルトの global_policy にクラスを追加して、すべてのインターフェイスに対してリダイレクトをイネーブルにすることもできます。新しいポリシーマップをグローバルに適用するのではなく、global_policy にクラスを追加して、デフォルトのグローバルポリシーの一部であるデフォルトのプロトコル インスペクションを削除してください。

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

**ステップ 8** サービス ポリシーを設定します。

クラウド Web セキュリティに別のポリシー マップを作成した場合に、それをインターフェイスに適用する例を次に示します。クラスを global_policy マップに追加した場合には、これで完了となるため、service-policy コマンドを入力する必要はありません。

```
hostname(config)# service-policy pmap-webtraffic interface inside
```

# アイデンティティ ファイアウォールの Active Directory 統合の例

次に、Active Directory 統合のエンドツーエンドの設定例を示します。この設定は、アイデンティティ ファイアウォールをイネーブルにします。

**手順**

**ステップ 1** LDAP を使用する Active Directory サーバを設定します。

次に、LDAP を使用して ASA で Active Directory サーバを設定する例を示します。

```
hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn
cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1
```

**ステップ 2** RADIUS を使用する Active Directory エージェントを設定します。

次に、RADIUS を使用して ASA で Active Directory エージェントを設定する例を示します。

```
hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent
```

**ステップ 3** （AD エージェント サーバで）AD エージェント サーバのクライアントとして ASA を作成します。

次に、Active Directory エージェント サーバのクライアントとして ASA を作成する例を示します。

```
c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123
```

**ステップ 4** （AD エージェント サーバで）AD エージェントと DC の間にリンクを作成します。

次に、ログオン/ログオフ イベントをモニタする Active Directory エージェントとすべての DC の間にリンクを作成する例を示します。

```
c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC
-domain W2K3DC.asascanlab.local -user administrator -password Password1
c:\IBF\CLI\adacfg.exe dc list
```

最後のコマンドを実行すると、ステータス「UP」が表示されます。

AD_Agent がログオン/ログオフ イベントをモニタするには、アクティブにモニタされているすべての DC でこれらのイベントがログに記録されていることを確認する必要があります。これを行うには、次を選択します。

**[Start] > [Administrative Tools] > [Domain Controller Security Policy]**

**[Local policies] > [Audit Policy] > [Audit account logon events (success and failure)]**

**ステップ 5** （ASA に戻ります）AD エージェントをテストします。

次に、ASA と通信できるようにテスト Active Directory エージェントを設定する例を示します。

```
hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)
INFO: Ad-agent Successful
```

コマンド「**show user-identity ad-agent**」も参照してください。

**ステップ 6** ASA でアイデンティティ オプションを設定します。

次に、ASA でアイデンティティ オプションを設定する例を示します。

```
hostname(config)# user-identity domain ASASCANLAB aaa-server AD
hostname(config)# user-identity default-domain ASASCANLAB
```

**ステップ 7** ユーザ アイデンティティ オプションを設定し、詳細なレポートをイネーブルにします。

次に、ASA にユーザ クレデンシャルを送信し、プロキシ サーバからの詳細なユーザ レポートをイネーブルにするユーザ アイデンティティ オプションを設定する例を示します。

```
hostname(config)# user-identity inactive-user-timer minutes 60
hostname(config)# user-identity action netbios-response-fail remove-user-ip
hostname(config)# user-identity user-not-found enable
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download
```

アイデンティティ ファイアウォールには、フル ダウンロードおよびオンデマンドの 2 つのダウンロード モードがあります。

- フル ダウンロード：ユーザがネットワークにログインするたびに、IDFW は即時に ASA にユーザ アイデンティティを通知します（ASA 5512-X 以降で推奨）。
- オンデマンド：ユーザがネットワークにログインするたびに、ASA が AD からユーザ アイデンティティを要求します。

複数のドメインを使用する場合は、次のコマンドを入力します。

hostname(config)# **user-identity domain** *OTHERDOMAINNAME*

**ステップ 8** Active Directory グループをモニタします。

次に、Active Directory グループをモニタするように設定する例を示します。

```
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME3
```

完了後に設定を保存するようにしてください。

**ステップ 9** Active Directory サーバからアクティブ ユーザ データベース全体をダウンロードします。

次のコマンドは、ポーリング インポート ユーザ グループ タイマーの満了を待たずに即時に Active Directory サーバを照会して、指定されたインポート ユーザ グループ データベースを更新します。

```
hostname(config)# user-identity update import-user
```

**ステップ 10** AD エージェントからデータベースをダウンロードします。

次に、ユーザ データベースが Active Directory と同期していないと思われる場合に、Active Directory エージェントからのデータベースのダウンロードを手動で開始する例を示します。

```
hostname(config)# user-identity update active-user-database
```

**ステップ 11** アクティブ ユーザのリストを表示します。

```
hostname# show user-identity user active list detail
```

# 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。<br>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。<br>**class-map type inspect scansafe**、**default user group**、**http[s]**（パラメータ）、**inspect scansafe**、**license**、**match user group**、**policy-map type inspect scansafe**、**retry-count**、**scansafe**、**scansafe general-options**、**server** {**primary** \| **backup**}、**show conn scansafe**、**show scansafe server**、**show scansafe statistics**、**user-identity monitor**、**whitelist** の各コマンドが導入または変更されました。 |

| 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。<br><br>**health-check application url** および **health-check application timeout** コマンドが追加されました。 |