CHAPTER 60

Cisco クラウド Web セキュリティ用の ASA の設定

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

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

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

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

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

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

この章の内容は、次のとおりです。

Cisco クラウド Web セキュリティについて

この項では、次のトピックについて取り上げます。

クラウド Web セキュリティへの Web トラフィックのリダイレクト

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

ユーザ認証およびクラウド Web セキュリティ

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

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

- AAA ルール：ASA が AAA ルールを使用してユーザ認証を実行すると、ユーザ名が AAA サーバまたはローカル データベースから取得されます。AAA ルールによるアイデンティティには、グループ情報が含まれていません。設定されている場合は、デフォルトのグループが使用されます。AAA ルールの設定については、第 44 章「ネットワーク アクセスに対する AAA 規則の設定」を参照してください。
- IDFW：ASA が Active Directory（AD）で IDFW を使用すると、アクセス ルールなどの機能またはサービス ポリシーで ACL を使用するか、ユーザ アイデンティティ モニタを設定してユーザ アイデンティティ情報を直接ダウンロードして、ユーザやグループをアクティブ化したときに、AD エージェントからユーザ名およびグループが取得されます。

  IDFW の設定については、第 39 章「アイデンティティ ファイアウォールの設定」を参照してください。
- デフォルトのユーザ名とグループ：ASA は、ユーザ認証を使用せずに、クラウド Web セキュリティ サービス ポリシー ルールと一致するすべてのユーザのオプションのデフォルトのユーザ名やグループを使用します。

認証キー

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

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

- 「企業認証キー」（P.60-3）
- 「グループ認証キー」（P.60-3）

企業認証キー

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

グループ認証キー

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

- 1 つの ASA のクラウド Web セキュリティ サービスをイネーブルにします。

- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

ポリシーにグループ認証キーを使用する方法については、「ScanCenter ポリシー」（P.60-4）を参照してください。

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

ScanCenter ポリシー

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

- 「ディレクトリ グループ」（P.60-4）
- 「カスタム グループ」（P.60-4）
- 「グループおよび認証キーの相互運用の仕組み」（P.60-5）

ディレクトリ グループ

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

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

- IDFW グループ名は次の形式で送信されます。

  *domain-name**group-name*

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

- デフォルト グループ名は次の形式で送信されます。

  [*domain*\]*group-name*

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

カスタム グループ

カスタム グループは、次の 1 つ以上の基準を使用して定義されます。

- ScanCenter グループ認証キー：カスタム グループのグループ認証キーを生成できます。その後、ASA を設定するときにこのグループ キーを識別すると、ASA からのすべてのトラフィックがグループ キーでタグ付けされます。
- 送信元 IP アドレス：カスタム グループの送信元 IP アドレスを特定できます。ASA サービス ポリシーが送信元 IP アドレスに基づくため、代わりに ASA で IP アドレスベースのポリシーを設定することもできます。
- ユーザ名：カスタム グループのユーザ名を識別できます。
  - IDFW ユーザ名は次の形式で送信されます。

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

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

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

    [*domain-name*\]*username*

    たとえば、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。

クラウド Web セキュリティのアクション

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

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

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

ホワイトリストを使用したスキャンのバイパス

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

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

IPv4 および IPv6 のサポート

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

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

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

クラス マップ トラフィック	クラウド Web セキュリティ インスペクション
IPv4 から IPv6	未サポート
IPv6 から IPv6	未サポート

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

Cisco クラウド Web セキュリティ サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。これらのサーバは、アベイラビリティをチェックするために定期的にポーリングされます。ASA がクラウド Web セキュリティ プロキシ サーバに到達することができない場合（SYN/ACK パケットがプロキシ サーバから到着しない場合など）、プロキシ サーバは TCP スリーウェイ ハンドシェイクを介してポーリングされて、アベイラビリティがチェックされます。設定した試行回数（デフォルトは 5）後に、プロキシ サーバが使用不可の場合、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。

継続ポーリングによってプライマリ サーバが連続する 2 回の再試行回数の期間にアクティブであることが示されると、ASA はバックアップ サーバからプライマリ クラウド Web セキュリティ プロキシ サーバに自動的にフォール バックします。CLI または ASDM を使用してこのポーリング間隔を変更できます。設定については、「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」（P.60-9）を参照してください。

プロキシ サーバが到達可能でないトラフィック状態	サーバ タイムアウトの計算	接続タイムアウトの結果
トラフィックが多い	クライアントのハーフ オープンの接続のタイムアウト + ASA TCP 接続タイムアウト	（30 + 30）= 60 秒
単一接続の失敗	クライアントのハーフ オープンの接続のタイムアウト +（（再試行しきい値 - 1）x（ASA TCP 接続タイムアウト））	（30 +（（5-1）X（30））） = 150 秒
アイドル：接続は送信されていません。	15 分 +（（再試行しきい値）x（ASA TCP 接続タイムアウト））	900 +（5 x（30））= 1050 秒

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
すべてのモデル	ASA とクラウド Web セキュリティ サーバ間のトラフィックを暗号化する高度暗号化（3DES/AES）ライセンス。

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

クラウド Web セキュリティの前提条件

（任意）ユーザ認証の前提条件

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

- AAA ルール（ユーザ名のみ）：第 44 章「ネットワーク アクセスに対する AAA 規則の設定」を参照してください。
- IDFW（ユーザ名とグループ）：第 39 章「アイデンティティ ファイアウォールの設定」を参照してください。

（任意）完全修飾ドメイン名の前提条件

サービス ポリシー ルールまたはクラウド Web セキュリティ サーバに対して ACL で FQDN を使用する場合は、「DNS サーバの設定」（P.15-11）に従って ASA の DNS サーバを設定する必要があります。

注意事項と制限事項

コンテキスト モードのガイドライン

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

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

各コンテキストには、必要に応じて独自の認証キーを設定できます。

ファイアウォール モードのガイドライン

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

IPv6 のガイドライン

IPv6 はサポートされません。「IPv4 および IPv6 のサポート」（P.60-6）を参照してください。

その他のガイドライン

- クラウド Web セキュリティは、ASA クラスタリングではサポートされません。
- クライアントレス SSL VPN はクラウド Web セキュリティではサポートされません。クラウド Web セキュリティの ASA サービス ポリシーからクライアントレス SSL VPN トラフィックを免除してください。
- クラウド Web セキュリティ プロキシ サーバへのインターフェイスがダウンすると、**show scansafe server** コマンドは、約 15 ～ 25 分間、両方のサーバを示します。この状態が発生する原因は、ポーリング メカニズムがアクティブな接続に基づいていること、また、そのインターフェイスがダウンしており、ゼロ接続を示し、ポーリング時間が最も長い方法が使用されることなどです。
- クラウド Web セキュリティは、ASA CX モジュールではサポートされません。同じトラフィックに対して ASA CX アクションおよびクラウド Web セキュリティ インスペクションの両方を設定した場合、ASA は ASA CX アクションのみを実行します。
- クラウド Web セキュリティ インスペクションは同じトラフィックの HTTP インスペクションと互換性があります。HTTP インスペクションは、デフォルト グローバル ポリシーの一部としてデフォルトでイネーブルになっています。

- クラウド Web セキュリティは、別の接続に対して同じ送信元ポートおよび IP アドレスを使用できる可能性がある拡張 PAT またはアプリケーションではサポートされません。たとえば、2 つの異なる接続（別個のサーバへの接続）が拡張 PAT を使用する場合、これらの接続は別個の宛先によって区別されているため、ASA は、両方の接続変換に同じ送信元 IP および送信元ポートを再利用する可能性があります。ASA がこれらの接続をクラウド Web セキュリティ サーバにリダイレクトすると、宛先がクラウド Web セキュリティ サーバの IP アドレスおよびポート（デフォルトは 8080）に置き換えられます。その結果、接続は両方とも、同じフロー（同じ送信元 IP/ ポートおよび宛先 IP/ ポート）に属しているように見え、リターン トラフィックが適切に変換解除されません。
- **match default-inspection-traffic** コマンドには、クラウド Web セキュリティ インスペクション用のデフォルト ポートは含まれません（80 および 443）。

デフォルト設定

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

Cisco クラウド Web セキュリティ の設定

クラウド Web セキュリティ プロキシ サーバとの通信の設定

ガイドライン

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

手順の詳細

	コマンド	目的
ステップ 1	**scansafe general-options** **例：** `hostname(config)# scansafe general-options`	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。
ステップ 2	**server primary** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **例：** `hostname(cfg-scansafe)# server primary ip 192.168.43.10`	プライマリ クラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。 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。

	コマンド	目的
ステップ 3	**server backup** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] **例：** hostname(cfg-scansafe)# server backup fqdn server.example.com	（任意）バックアップ クラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。 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。
ステップ 4	**retry-count** *value* **例：** hostname(cfg-scansafe)# retry-count 2	再試行回数値を入力します。この値は、アベイラビリティをチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。有効な値は 2 ～ 100 で、デフォルトは 5 です。 ASA は、最初にプライマリ サーバをチェックします。失敗した場合は、アクティブなプロキシ サーバとしてバックアップ サーバを使用します。連続する 2 回の再試行回数の期間に正常にアクティブである場合、ASA は自動的にプライマリ サーバにフォール バックします。
ステップ 5	**license** *hex_key* **例：** hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3	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。認証キーは 16 バイトの 16 進数です。 「認証キー」（P.60-3）を参照してください。

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
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

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

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。「セキュリティ コンテキストの設定」（P.6-20）を参照してください。

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
retry-count 5
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
!
```

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

サービス ポリシー ルールの詳細については、第 36 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。

前提条件

（任意）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「（任意）ホワイトリストに記載されたトラフィックを設定します」（P.60-16）に従ってホワイトリストを作成します。

手順の詳細

	コマンド	目的
ステップ 1	**policy-map type inspect scansafe** *name1* **例：** `hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1`	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。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。 *policy_map_name* 引数の長さは、最大 40 文字です。 ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 2	**parameters** **例：** `hostname(config-pmap)# parameters`	パラメータを使用すると、プロトコルおよびデフォルト ユーザまたはグループを設定できます。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。
ステップ 3	{**http** | **https**} **例：** `hostname(config-pmap-p)# http`	このインスペクション ポリシー マップには、**http** または **https** のいずれか 1 つのサービス タイプのみを指定できます。

	コマンド	目的
ステップ 4	（任意） **default** {[**user** *username*] [**group** *groupname*]} **例：** hostname(config-pmap-p)# default group default_group	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にデフォルトのユーザやグループが HTTP ヘッダーに含まれることを指定します。
ステップ 5	（任意。ホワイトリスト用） **class** *whitelist_name* **例：** hostname(config-pmap-p)# class whitelist1	「（任意）ホワイトリストに記載されたトラフィックを設定します」（P.60-16）で作成したホワイトリスト クラス マップ名を識別します。
ステップ 6	**whitelist** **例：** hostname(config-pmap-p)# class whitelist1 hostname(config-pmap-c)# whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。
ステップ 7	**policy-map type inspect scansafe** *name2* **parameters** **default** {[**user** *user*] [**group** *group*]} **class** *whitelist_name2* **whitelist** **例：** hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2 hostname(config-pmap)# parameters hostname(config-pmap-p)# default group2 default_group2 hostname(config-pmap-p)# class whitelist2 hostname(config-pmap-c)# whitelist	ステップ 1 ～ステップ 6 を繰り返して、HTTPS トラフィックの各クラス マップを作成します（例）。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 クラス マップを作成できます。必要に応じて、トラフィックの複数のクラスに対してインスペクション クラス マップを再利用できます。

	コマンド	目的
ステップ 8	**access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **tcp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] **例：** 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	クラウド Web セキュリティに送信するトラフィックのクラスを識別します。1 つまたは複数のアクセス コントロール エントリ（ACE）で構成される ACL を作成します。ACL の詳細については、第 20 章「拡張アクセス コントロール リストの追加」を参照してください。 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。したがって、HTTP のみの ACL および HTTPS のみの ACL を作成する必要があります。ポリシーに必要な数の ACL を作成します。 **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。 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。 *user_argument* を使用すると、インラインまたはオブジェクト グループを参照することにより、IDFW のユーザ名またはグループを指定できます。 *security_group_argument* を使用すると、インラインまたはオブジェクト グループを参照することにより、TrustSec セキュリティ グループを指定できます。セキュリティ グループによってクラウド Web セキュリティに送信するトラフィックを照合できますが、ASA はクラウド Web セキュリティの HTTP ヘッダーにセキュリティ グループ情報を送信しないことに注意してください。クラウド Web セキュリティはセキュリティ グループに基づいてポリシーを作成できません。
ステップ 9	**class-map** *name1* **例：** hostname(config)# class-map cws_class1	クラウド Web セキュリティ フィルテリングをイネーブルにするトラフィックを識別するためのクラス マップを作成します。
ステップ 10	**match access-list** *acl1* **例：** hostname(config-cmap)# match access-list SCANSAFE_HTTP	ステップ 8 で作成した ACL を指定します。 このルールには別の照合文を使用できますが、HTTP または HTTPS のみのトラフィックを識別する最も汎用的なコマンドである **match access-list** コマンドを使用することを推奨します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.36-12）を参照してください。

	コマンド	目的
ステップ 11	**class-map** *name2* 　**match access-list** *acl2* **例：** hostname(config)# class-map cws_class2 hostname(config-cmap)# match access-list SCANSAFE_HTTPS	（任意）HTTPS トラフィックなどのクラス マップを作成します。このサービス ポリシー ルールに必要な数のクラスを作成できます。
ステップ 12	**policy-map** *name* **例：** hostname(config)# policy-map cws_policy	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。デフォルトのグローバル ポリシーのグローバル マップは global_policy と呼ばれます。このポリシーを編集するか、または新しいポリシーを作成できます。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。
ステップ 13	**class** *name1* **例：** hostname(config-pmap)# class cws_class1	ステップ 9 で作成したクラス マップを識別します。
ステップ 14	**inspect scansafe** *scansafe_policy_name1* [**fail-open** | **fail-close**] **例：** hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。ステップ 1 で作成したインスペクション クラス マップの名前を指定します。 **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。
ステップ 15	**class** *name2* 　**inspect scansafe** *scansafe_policy_name2* [**fail-open** | **fail-close**] **例：** hostname(config-pmap)# class cws_class2 hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open	（任意）ステップ 11 で作成した 2 番目のクラス マップを識別し、そのマップに対するクラウド Web セキュリティ インスペクションをイネーブルにします。 必要に応じて複数のクラス マップを設定できます。
ステップ 16	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy cws_policy inside	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。**global** 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 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。詳細については、「インターフェイスへのアクションの適用（サービス ポリシー）」（P.36-17）を参照してください。

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
```

（任意）ホワイトリストに記載されたトラフィックを設定します

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

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

手順の詳細

	コマンド	目的
ステップ 1	**class-map type inspect scansafe** [**match-all** | **match-any**] *name* **例：** `hostname(config)# class-map type inspect scansafe match-any whitelist1`	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。 *class_map_name* 引数は、最大 40 文字のクラス マップ名です。 **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基準の 1 つに一致したらクラス マップと一致することを指定します。 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。
ステップ 2	**match** [**not**] {[**user** *username*] [**group** *groupname*]} **例：** `hostname(config-cmap)# match`	**match** キーワードには、特定のユーザ名またはグループ名が続きます。このキーワードは、ホワイトリストにユーザまたはグループを指定します。 **match not** キーワードはユーザや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、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
```

（任意）ユーザ アイデンティティ モニタを設定します

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

制約事項

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

手順の詳細

コマンド	目的
user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*} **例：** hostname(config)# user-identity monitor user-group CISCO\\Engineering	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。 • **user-group**：グループ名インラインを指定します。ドメインとグループの間に 2 つのバックスラッシュ（\\）を指定しますが、ASA は、クラウド Web セキュリティへの送信時に、クラウド Web セキュリティの表記規則に準拠するようにバックスラッシュが 1 つのみ含まれるように名前を変更します。 • **object-group-user**：**object-group user** 名を指定します。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。

クラウド Web セキュリティ ポリシーの設定

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

手順の詳細

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

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

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

クラウド Web セキュリティのモニタ

コマンド	目的
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の HTTP 接続を表示します。
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。
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。
次の URL を参照してください。 http://Whoami.scansafe.net	トラフィックがクラウド Web セキュリティ サーバに移動するかどうかを確認するには、クライアントからこの Web サイトにアクセスします。

show scansafe server コマンドは、クラウド Web セキュリティ プロキシ サーバが到達可能かどうかを示します。

```
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 コマンドは、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のクラウド 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 コマンドは、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
```

Cisco クラウド Web セキュリティの設定例

シングル モードの例

次に、Cisco クラウド Web セキュリティの完全な設定の例を示します。

アクセス リストの設定

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
```

クラス マップの設定

```
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
```

インスペクション ポリシー マップの設定

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

ポリシー マップの設定

```
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
```

サービス ポリシーの設定

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

ASA でのクラウド Web セキュリティの設定

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225 web 8080
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

マルチ モードの例

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、認証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例を示します。

```
!System Context
!
hostname(config)#scansafe general-options
hostname(cfg-scansafe)#server primary ip 180.24.0.62 port 8080
hostname(cfg-scansafe)#retry-count 5
hostname(cfg-scansafe)#license FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
hostname(cfg-scansafe)#publickey <path to public key>
!
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 366C1D3F5CE67D33D3E9ACEC265261E5
!
config-url disk0:/two_ctx.cfg
!
```

ホワイトリストの例

どのアクセス リスト トラフィックをクラウド Web セキュリティに送信する必要があるかを設定します。

```
access-list 101 extended permit tcp any4 any4 eq www
access-list 102 extended permit tcp any4 any4 eq https

class-map web
 match access-list 101
class-map https
 match access-list 102
```

user1 がこのアクセス リストの範囲内であることを確認するホワイト リストを設定して、クラウド Web セキュリティをバイパスするには、次を実行します。

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

クラウド Web セキュリティ ポリシー マップにクラス マップを添付するには、次を実行します。

```
policy-map type inspect scansafe ss
 parameters
  default user user1 group group1
  http
 class whiteListCmap
 whitelist

policy-map type inspect scansafe ss2
 parameters
  default user user1 group group1
  https
 class whiteListCmap
 whitelist
```

このインスペクション ポリシーを作成したら、サービス グループに割り当てられるポリシー マップに添付します。

```
policy-map pmap
 class web
  inspect scansafe ss fail-close
class https
  inspect scansafe ss2 fail-close
```

次に、ポリシー マップをサービス ポリシーに添付して、グローバルに有効にするか、または ASA インターフェイスごとに有効にします。

```
service-policy pmap interface inside
```

ディレクトリの統合の例

この項では、ディレクトリの統合のさまざまな設定例を示します。第 39 章「アイデンティティ ファイアウォールの設定」も参照してください。

- 「LDAP を使用する Active Directory サーバの設定」（P.60-21）
- 「RADIUS を使用する Active Directory エージェントの設定」（P.60-22）
- 「AD エージェント サーバのクライアントとしての ASA の作成」（P.60-22）
- 「AD エージェントと DC の間のリンクの作成」（P.60-22）
- 「AD エージェントのテスト」（P.60-22）
- 「ASA のアイデンティティ オプションの設定」（P.60-23）
- 「ユーザ アイデンティティ オプションの設定および詳細なレポートのイネーブル化」（P.60-23）
- 「Active Directory グループのモニタリング」（P.60-23）
- 「Active Directory サーバからのアクティブ ユーザ データベース全体のダウンロード」（P.60-23）
- 「AD エージェントからのデータベースのダウンロード」（P.60-23）
- 「アクティブ ユーザのリストの表示」（P.60-23）

LDAP を使用する Active Directory サーバの設定

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
```

RADIUS を使用する Active Directory エージェントの設定

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
```

AD エージェント サーバのクライアントとしての ASA の作成

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
```

AD エージェントと DC の間のリンクの作成

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)]

AD エージェントのテスト

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。

ASA のアイデンティティ オプションの設定

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
```

ユーザ アイデンティティ オプションの設定および詳細なレポートのイネーブル化

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
```

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
```

Active Directory グループのモニタリング

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
```

注意　完了後に設定を保存するようにしてください。

Active Directory サーバからのアクティブ ユーザ データベース全体のダウンロード

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
```

AD エージェントからのデータベースのダウンロード

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
```

アクティブ ユーザのリストの表示

次に、アクティブなユーザを表示する例を示します。

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

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 5510 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 は AD（ADHOC）からのユーザ アイデンティティを要求します（メモリ制約のため ASA 5505 で推奨）。

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

次に、ASA でアイデンティティ ファイアウォールを使用するクラウド Web セキュリティを設定する例を示します。

```
hostname# sh run
ASA Version 100.8(24)32
!
hostname QFW-201-QASS
domain-name uk.scansafe.net
enable password liqhNWIOSfzvir2g encrypted
passwd liqhNWIOSfzvir2g encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.116.90 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 192.168.114.90 255.255.254.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa100824-32-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name uk.scansafe.net
object network obj0192.168.116.x
 subnet 192.168.116.0 255.255.255.0
access-list 101 extended permit tcp any any eq www
access-list 101 extended permit tcp any any eq https
access-list web extended permit tcp any any eq www
access-list icmp extended permit icmp any any
access-list https extended permit tcp any any eq https
```

```
!
scansafe general-options
 server primary ip 192.168.115.225 web 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC26789534f
!
pager lines 24
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
!
object network obj0192.168.116.x
 nat (inside,outside) dynamic interface
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.114.19 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
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
no snmp-server location
no snmp-server contact
crypto ca trustpool policy
telnet timeout 5
ssh 192.168.0.0 255.255.255.0 inside
ssh 192.168.21.0 255.255.255.0 inside
ssh timeout 30
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map cmap-https
 match access-list https
class-map inspection_default
 match default-inspection-traffic
```

```
class-map cmap-http
 match access-list web
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map type inspect scansafe ss
 parameters
  default user john group qa
  http
policy-map type inspect scansafe https-pmap
 parameters
  https
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map type inspect scansafe http-pmap
 parameters
  default group http-scansafe
  http
policy-map pmap-http
 class cmap-http
  inspect scansafe http-pmap fail-open
 class cmap-https
  inspect scansafe https-pmap fail-open
!
service-policy pmap-http global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:667ba936945b370c394806a63548e7a0
: end
QFW-201-QASS#
```

関連資料

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

Cisco クラウド Web セキュリティの機能の履歴

表 60-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 60-1　クラウド Web セキュリティ の機能の履歴

機能名	プラットフォーム リリース	機能情報
クラウド Web セキュリティ	9.0(1)	この機能が導入されました。 Cisco クラウド Web セキュリティは、Web トラフィックに対するコンテンツ スキャンおよびその他のマルウェア保護サービスを提供します。また、ユーザ アイデンティティに基づいて Web トラフィックのリダイレクトと報告を行うこともできます。 **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。