ScanSafe Web Security の使用

Security Manager により、ScanSafe Web Security との統合が可能になります。ScanSafe Web Security は、クラウド ベースの SaaS（Security as a Service）機能であり、Web セキュリティ データセンターを世界中のさまざまな場所で利用できるようになります。ScanSafe Web Security とルータを統合すると、他の方法によるコンテンツ スキャンおよびマルウェアの検出のために、選択した HTTP トラフィックと HTTPS トラフィックが ScanSafe Cloud にリダイレクトされます。また、ScanSafe Web Security を使用して特定のユーザ、ユーザ グループ、および IP にディファレンシエーテッド サービスも提供できます。

Security Manager から ScanSafe Web Security を起動すると、次の領域のポリシーおよび設定を定義できます。

- コンテンツ スキャン設定
- コンテンツ スキャン ポリシー
- AAA サーバ設定
- AAA ポリシー

Security Manager で ScanSafe Web Security を統合することにより、ほぼすべてのポリシーおよびフレームワーク ベースのポリシー機能をコピーおよび共有できます。次の表で、スキャンおよび AAA ポリシー タイプのサポート範囲について詳しく説明します。

サポートされるタイプ	例
コンテンツスキャン設定	プライマリ サーバ IP、セカンダリ サーバ IP、サーバ タイムアウト
コンテンツ スキャン ポリシー	グローバル許可リストポリシー ユーザ グループの追加または除外、デフォルト ユーザ設定、デフォルト ユーザ グループの設定 コンテンツ スキャンをイネーブルする必要があるインターフェイス

サポートされるタイプ	例
AAA サーバー設定	HTTP Basic および NTLM ポリシーで使用されるアイデンティティ ポリシー オブジェクト HTTP Basic および NTLM に関連するタイムアウト プロキシ、HTTP Basic、および NTLM の発生順序 IOS の LDAP サーバーおよび LDAP 属性マップ設定 （注） また、RADIUS サーバおよび TACAS サーバもサポートされています。 インターフェイスごとの AAA リスト
AAA ポリシー	HTTP Basic および NTLM アドミッションルールのサポート（認証方式）が、以前から使用可能な認証プロキシ方式に追加されました。

Security Manager は、次の機能をサポートしていません。

- http/https の検査ルールまたは ZBF ルールが存在しない場合の PAM 設定
- 古い IOS バージョンで LDAP を使用する認証プロキシ（ScanSafe Web Security をサポートする IOS バージョンでのみ可能）
- AAA 方式としての AuthProxy によるアイデンティティ ポリシー。（NTLM および HTTP Basic のみをサポートしています）
- アイデンティティ ポリシーを作成するための Virtual Template 番号の検証
- LDAP サーバ用の Secure Trust Point の検証
- コンテンツスキャンルールの継承
- ユーザーグループおよびユーザーの AD ブラウジング
- 新しいポリシー（ポリシー クエリーなど）に対するツール サポート
- 制御タグポリシー

ScanSafe Web セキュリティ製品の詳細については、http://www.cisco.com/en/US/partner/products/ps11720/index.html を参照してください。

この章は、次のセクションで構成されています。

- ScanSafe Web セキュリティの設定 （3 ページ）
- ScanSafe Web Security ページ （5 ページ）
- [ScanSafe Web Security Settings] ページ （8 ページ）

ScanSafe Web セキュリティの設定

[ScanSafe Web Security設定（ScanSafe Web Security Settings）] ページを使用して、デフォルトのユーザグループの設定を定義します。他の設定ポリシーと同様に、デフォルトのユーザグループ ポリシー設定を共有できます。

関連項目

- ScanSafe Web Security ページ （5 ページ）
- [ScanSafe Web Security Settings] ページ （8 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （7 ページ）
- [AAA Rules] ページ

（注） すべての手順は、ポリシービューから実行されたものとして表示されます。

ScanSafe Web セキュリティを設定するには、次の手順を実行します。

ステップ 1 ポリシータイプセレクタから、[ファイアウォール（Firewall）]、[ScanSafe Webセキュリティ（ScanSafe Web Security）] の順に選択します。 >

[ScanSafe Web Security] ページが表示され、[Interfaces] タブが選択されています。

ステップ 2 Web リクエストを ScanSafe Web セキュリティサーバーに転送するために使用するインターフェイスを、[利用可能なインターフェイス（Available Interfaces）] 列のリストから選択して、[選択したインターフェイス（Selected Interfaces）] 列に移動することにより、有効にします。

ステップ 3 [正規表現の許可リスト（Permitlisting Regular Expressions）] タブを選択します。

ステップ 4 通知を許可リストに関する ScanSafe Web セキュリティサーバーに送信するには、[通知タワー（Notify Tower）] チェックボックスをオンにします。これは、IP ベースのものを除くすべての許可リストに適用できます。

（許可リストに正規表現が指定されていない場合、ScanSafe Web セキュリティは警告を受け取ります。）

ステップ 5 HTTP ホストエリアで、[利用可能な正規表現（Available Regular Expressions）] カラムのリストから正規表現を選択し、[選択した正規表現（Selected Regular Expressions）] カラムに移動することにより、（正規表現マッチングを使用して）許可される正規表現を指定します。

ステップ 6 HTTP ユーザーエージェントエリアで、[利用可能な正規表現（Available Regular Expressions）] カラムのリストから正規表現を選択し、[選択した正規表現（Selected Regular Expressions）] カラムに移動することにより、許可される正規表現を指定します。

ステップ 7 [許可リストACL（Permitlisting ACLs）] タブを選択します。

ステップ 8 タイプリストから [拡張（Extended）] または [標準（Standard）] を選択して、操作する ACL のタイプを指定します。

ステップ 9 許可リストに追加する ACL を指定するには、左側の列のリストから ACL を選択し、それらを [選択したアイテム（Selected items）] カラムに移動します。

ステップ 10 [ユーザーグループ（User Groups）] タブを選択します。

ヒント [ユーザーグループ（User Groups）] ページを使用して、ユーザーグループを定義し、デフォルトユーザとデフォルトユーザーグループの両方を指定し、ユーザーグループを含めたり除外したりできます。これら 3 つのリストすべてのエントリを編集または削除することもできます。

ステップ 11 [デフォルトユーザ（Default User）] フィールドにユーザ名を入力して、デフォルトユーザを指定します（任意）。

ステップ 12 [デフォルトユーザーグループ（Default User Group）] フィールドにユーザーグループ名を入力して、デフォルトユーザーグループを指定します。

ステップ 13 インターフェイスを選択し、ユーザーグループを [含める（Include）] リストに追加して、ユーザーグループを含めます。

ステップ 14 インターフェイスを選択し、ユーザーグループを [除外（Exclude）] リストに追加して、ユーザーグループを除外します。

ステップ 15 ポリシーセレクタから [ポリシー（Policy）] > [ファイアウォール（Firewall）] > [設定（Settings）] > [ScanSafe Webセキュリティ（ScanSafe Web Security）] を選択します。

ステップ 16 [詳細（Details）] タブを選択し、次の値を入力してプライマリ ScanSafe サーバーを指定します。

- IP アドレス/名前（IP Address/Name）
- HTTP ポート（デフォルトは 8080）
- HTTPS ポート（デフォルトは 8080）

ステップ 17 [詳細（Details）] タブを選択し、次の値を入力してセカンダリ ScanSafe サーバーを指定します。

- IP アドレス/名前（有効な IP アドレスまたは FQDN のみ）。
- HTTP ポート（デフォルトは 8080）
- HTTPS ポート（デフォルトは 8080）

ステップ 18 [サーバーのタイムアウト（Server Timeout）] 期間を秒で指定します（デフォルトは 300）。

ステップ 19 [セッションアイドルタイムアウト（Session Idle Timeout）] 期間を秒で指定します（デフォルトは 300）。

ステップ 20 次のいずれか *1* つを実行して、送信元アドレスを指定します。

- [IPアドレス（IP Address）] ボタンをクリックし、IP アドレスを入力します。
- [インターフェイス（Interface）] ボタンをクリックし、[選択（Select）] ボタンをクリックして、インターフェイスセレクタを参照してインターフェイスを選択します。

（注） 有効なソース IP またはインターフィエスは、ScanSafe Web セキュリティが有効になっているインターフェイスの 1 つである必要があります（[ファイアウォール（Firewall）] > [ScanSafe Webセキュリティ（ ScanSafe Web Security）] ページ > [インターフェイス（Interface）] タブで）。

ステップ 21 **ライセンス**を入力し、暗号化されている場合はチェックボックスをオンにします。

ヒント [暗号化（Encrypted ）] が選択されていない場合、入力する値は 32 文字の 16 進数にする必要があります。

ステップ 22 必要に応じて、[ログの有効化（Enable Logging）] チェックボックスをオンにします。

ScanSafe Web Security ページ

Security Manager により、ScanSafe Web Security との統合が可能になります。ScanSafe Web Security は、クラウド ベースの SaaS（Security as a Service）機能であり、Web セキュリティ データセンターを世界中のさまざまな場所で利用できるようになります。ScanSafe Web Security とルータを統合すると、他の方法によるコンテンツ スキャンおよびマルウェアの検出のために、選択した HTTP トラフィックと HTTPS トラフィックが ScanSafe Cloud にリダイレクトされます。また、ScanSafe Web Security を使用して特定のユーザ、ユーザ グループ、および IP にディファレンシエーテッド サービスも提供できます。

Security Manager で ScanSafe Web セキュリティを使用すると、次の領域の設定およびポリシーを定義できます。

- コンテンツ スキャン設定
- コンテンツ スキャン ポリシー
- AAA サーバ設定
- AAA ポリシー

Security Manager で ScanSafe Web Security を統合することにより、ほぼすべてのポリシーおよびフレームワーク ベースのポリシー機能をコピーおよび共有できます。

ナビゲーション パス

（ポリシー ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

（注） ScanSafe Web セキュリティのポリシーと設定は、マップ ビューを使用して設定することもできます。

関連項目

- ScanSafe Web セキュリティの設定 （3 ページ）
- [ScanSafe Web Security Settings] ページ （8 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （7 ページ）

- [AAA Rules] ページ

フィールド リファレンス

要素	説明
[インターフェイス（Interfaces）] タブ	
：フィルタ（Filter）	Security Manager でのフィルタの使用方法の詳細については、テーブルのフィルタリングを参照してください。
インターフェイス	このタブでは、コンテンツスキャンのために Web 要求が ScanSafe Web セキュリティサーバーに転送されるインターフェイスおよび Security Manager 定義のインターフェイスロールを選択できます。
— Available Interfaces	ScanSafe Web Security 用に選択可能なインターフェイス。
— 選択されたインターフェイス（Selected Interfaces）	選択されたインターフェイスは、Web サービスに対するホストの要求が ScanSafe Web セキュリティサーバーに転送される WAN に面している必要があります。
-	-
[正規表現の許可リスト（Permitlisting Regular Expressions）] タブ	
— Notify Tower	このチェックボックスをオンにすると、許可リストに関して ScanSafe Web セキュリティタワーに通知する必要があることを指定します。これは、IP ベースの許可リストを除く、すべての ACL ベースの許可リストのバリエーションに適用されます。デフォルトの動作では、通知は送信されません。
— Available Regular Expressions (HTTP Host)	ScanSafe Web Security サーバへの配信で使用可能であり、検討対象となる正規表現をリストします。
—フィルター（Filter）（HTTP ホスト）	管理者は、ユーザーグループリストの包含および除外を指定することにより、ScanSafe Web セキュリティサーバーに送信される許可された正規表現をフィルタリングできます。このフィルタは、[Match All] または [Match Any] のいずれかで操作します。
— Selected Regular Expressions (HTTP Host)	選択した正規表現に一致するホストは許可リストに追加され、ScanSafe Web セキュリティサーバーにリダイレクトされません。
— Available Regular Expressions (HTTP User Agent)	使用可能な正規表現に一致するエージェントは許可リストに追加され、ScanSafe Web セキュリティサーバーにリダイレクトされません。

要素	説明
— 選択された正規表現（Selected Regular Expressions）（HTTP ホスト）	設定すると、[選択された正規表現（Selected Regular Expressions）] リストにある正規表現のみが ScanSafe クラウドに送信されます。
[許可リストACL（Permitlisting ACLs）] タブ	
— ACL タイプ（ACL Type）	ACL許可リストのタイプ（標準または拡張のいずれか）を指定します。 （注） 許可リストに使用される標準 ACL は、拡張 ACL として検出されます。ACL名に「CSM_EXT_」のプレフィックスが付加されます。拡張 ACL は完全であり推奨されるため、標準 ACL は拡張 ACL に変換されます
— 選択された ACLS（Selected ACLS）	設定すると、[選択された正規表現（Selected Regular Expressions）] リストにある正規表現のみが ScanSafe クラウドに送信されます。
[User Groups] タブ	
— デフォルトユーザー（Default User）	コンテンツ スキャン セッションに固有のユーザ名がない場合、ScanSafe Web Security サーバに送信されるグローバル名。たとえば、支社内のすべてのユーザに対して、同じコンテンツ スキャン ポリシーを適用する場合に使用します。
— Default User Group	コンテンツ スキャン セッションに固有のユーザ名がない場合、ScanSafe Web Security サーバに送信されるグローバル名。たとえば、支社内のすべてのユーザ グループに対して、同じコンテンツ スキャン ポリシーを適用する場合に使用します。
— インターフェイス固有のデフォルト ユーザー グループ（Interface Specific Default User Groups）	各インターフェイスのデフォルトのユーザーグループを一覧表示します。
— 包含（Include）/除外（Exclude）	包含リストまたは除外リストを使用して、包含または除外する特定のユーザーグループを指定できます。

[Add Default User Group]/[Edit Default User Group] ダイアログボックス

特定のインターフェイスのデフォルト ユーザ グループを指定するには、[Default User Groups] ダイアログボックスを使用します。

これらの ScanSafe Web Security サーバーの設定の詳細については、[ScanSafe Web Security Settings] ページ （8 ページ）を参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- ScanSafe Web Security ページ （5 ページ）
- [ScanSafe Web Security Settings] ページ （8 ページ）
- ScanSafe Web セキュリティの設定 （3 ページ）
- [AAA Rules] ページ

ナビゲーション パス

（ポリシー ビュー）[Firewall] を選択し、[ScanSafe Web Security] ページを開きます。次に [User Groups] タブをクリックします。

[ScanSafe Web Security Settings] ページ

関連項目

- ScanSafe Web Security ページ （5 ページ）
- ScanSafe Web セキュリティの設定 （3 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （7 ページ）
- [AAA Rules] ページ

ナビゲーション パス

（ポリシー ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

（デバイス ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

フィールド リファレンス

表 *1 : ScanSafe Web Security* の設定

要素	説明（**Description**）	使用方法
IP Address|Name (Primary ScanSafe Server)	ScanSafe Web Security を操作するために設定されたサーバのプライマリ FQDN または IP アドレス。	両方
HTTP Port (Primary ScanSafe Server)	プロキシ HTTP トラフィック用のデフォルト プライマリ ポート（デフォルトは 8080）。	両方
[HTTPS ポート（プライマリ ScanSafe サーバー）（HTTPS Port (Primary ScanSafe Server)）]	プロキシ HTTPS トラフィック用のデフォルトプライマリポート（デフォルトは 8080）。	両方
[IP アドレス/名前（バックアップ ScanSafe サーバー）（IP Address/Name (Backup ScanSafe Server)）]	ScanSafe Web Security を操作するために設定されたサーバーのセカンダリ FQDN または IP アドレス。	両方
[HTTP ポート（バックアップ ScanSafe サーバー）（HTTP Port (Backup ScanSafe Server)）]	プロキシ HTTP トラフィック用のデフォルト セカンダリ ポート（デフォルトは 8080）。	両方
[HTTPS ポート（セカンダリ ScanSafe サーバー）（HTTPS Port (Secondary ScanSafe Server)）]	プロキシ HTTPS トラフィック用のデフォルトセカンダリポート（デフォルトは 8080）。	両方
サーバー タイムアウト（Server timeout）	ScanSafe Web セキュリティサーバーの可用性をチェックするときのポーリングタイムアウト。	IOS のみ
セッション アイドル タイムアウト（Session Idle Timeout）	ScanSafe Web セキュリティサーバーの非アクティブタイムアウト（デフォルトは 300 秒）。セッションが非アクティブであることが検出された場合にセッションを削除するために使用されます。	IOS のみ
On Failure	プライマリとセカンダリの両方の ScanSafe Web Security サーバが非アクティブであることを検出した場合に、実行する処置（すべてのトラフィックをドロップする、またはすべてのトラフィックを通過させる）を決定します。	IOS のみ
IP Address (Source Address)	ScanSafe Web Security サーバへのパケットがルータから送信される際の、送信元の IP アドレス。	IOS のみ

要素	説明（**Description**）	使用方法
Interface (Source Address)	ScanSafe Web Security サーバへのパケットがルータから送信される際の、送信元のインターフェイス アドレス。	IOS のみ
ライセンス	ScanSafe Web Security サーバに送信されたライセンス（32 文字の 16 進数）	Both
Encrypted	選択すると、暗号化がイネーブルになります。ASA は、暗号化されたライセンステキストの設定を受け入れません。	IOS のみ
Enable Logging Checkbox	IOS syslogs をイネーブルにします（デフォルトでは、イネーブルされません）。	IOS のみ
[公開キーファイル（Public Key File）]	公開キーファイルの名前。	ASA のみ
[接続再試行回数（Connection Retry Count）]	システムが接続を再試行する回数。	ASA のみ

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。