はじめに

この章で説明する内容は、次のとおりです。

Secure Web Appliance について

Cisco Secure Web Appliance（SWA）はインターネットトラフィックを代行受信してモニターし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネットベースの脅威から内部ネットワークを保護します。Cisco Secure Web Appliance はプロキシサーバーとして機能し、ユーザーからの Web 要求を代行受信して、要求された Web コンテンツをスキャンし、マルウェア、ウイルス、フィッシング攻撃などの潜在的な脅威を検出します。URL フィルタリング、ウイルス対策スキャン、レピュテーションベースのフィルタリング、高度なマルウェア防御などのさまざまなセキュリティテクノロジーを使用して、Web トラフィックのセキュリティを確保します。全体として、 Secure Web Appliance は、組織が Web トラフィックを保護し、使用ポリシーを適用し、Web ベースの脅威から保護するのに役立ち、より安全で制御された Web ブラウジング環境をユーザーに提供します。

AsyncOS 15.0 の新機能

表 *1 : AsyncOS 15.0* の新機能

機能	説明
スマート ソフトウェア ライセンシングの機能強化	スマート ソフトウェア ライセンシング機能に加えられた拡張機能は次のとおりです。 • ライセンス予約：Cisco Smart Software Manager（CSSM）ポータルに接続せずに、Cisco Secure Web Appliance で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Web Appliance を展開するユーザーにとって有益です。 詳細については、概要および機能ライセンスの予約を参照してください。 • Device Led Conversion（DLC）：Cisco Secure Web Appliance をスマートライセンスに登録すると、既存の有効なクラシックライセンスはすべて、Device Led Conversion（DLC）プロセスを使用して自動的にスマートライセンスに変換されます。これらの変換されたライセンスは、CSSM ポータルのバーチャルアカウントで更新されます。 「概要」を参照してください。 （注） • AsyncOS バージョン 15.0 は、クラシックライセンスがサポートされる最後のリリースです。AsyncOS の次のメジャーリリースでは、スマートライセンスのみがサポートされます。 • AsyncOS バージョン 15.0 は、Sx90/F モデルでサポートされる最後のリリースになります。
詳細な帯域幅制御	クォータプロファイルで帯域幅の値を設定し、暗号化ポリシーおよびアクセスポリシー URL カテゴリまたは全体的な Web アクティビティ クォータでクォータプロファイルをマッピングすることにより、トラフィックの帯域幅を管理できます。 時間、ボリューム、および帯域幅のクォータの定義を参照してください。

機能	説明
ポリシーの複製	ポリシーの複製機能を使用すると、ポリシーの既存の構成をコピーまたは複製して、新しいポリシーを作成できます。 「ポリシーの設定」を参照してください。
アプリケーションの検出および制御（ADC）エンジン	サポートされるADC エンジンは、アクセプタブル ユース ポリシーのコンポーネントであり、アプリケーションで使用されるWebトラフィックを深く理解し、管理できるように、Webトラフィックを検査します。 AsyncOS 15.0 以降では、AVC または ADC エンジンを使用して Web トラフィックを監視できます。デフォルトでは、AVC は有効になっています。ADC エンジンは、高性能モードをサポートします。 URL フィルタリング エンジンの設定およびポリシーの設定を参照してください。
ADC 設定用の REST API	設定情報を取得し、変更（既存の情報の変更、新しい情報の追加、エントリの削除など）を、REST API を使用してアプライアンスのアクセスポリシー設定データで実行できます。 『AsyncOS API 15.0 for Cisco Secure Web Appliance - Getting Started Guide』を参照してください。
拡張機能	
SNMP3 のデフォルト以外のユーザー名	AsyncOS 15.0 以降、管理者は、デフォルトユーザー名 [v3get] 以外のカスタム SNMPv3 ユーザ名の設定を選択できます。 SNMP を使用したシステムの状態のモニタリングを参照してください。
カスタムヘッダー	カスタムヘッダーの最大長は 16k です。 Web 要求へのカスタム ヘッダーの追加を参照してください。
安全なトンネルインターフェイスとリモートアクセス接続を選択するオプション	トンネルとリモート アクセス接続の確立に使用するインターフェイスを選択できます。 アプライアンスへのリモート アクセスのイネーブル化を参照してください。

機能	説明
プラットフォームのアップグレード	AsyncOS 15.0 から、FreeBSD バージョンが FreeBSD 13.0 にアップグレードされました。 以下がアップグレードされました。 • Cisco SSL バージョン 1.0.2 から Cisco SSL バージョン 1.1.1。 • AVC、WBRSD、DCA、Beaker などの Talos エンジンがアップグレードされました。 • Webroot や McAfee などのスキャナエンジンがアップグレードされました。 （注） FreeBSD 13.0 は、Cisco SSL バージョン 1.1.1 のみと互換性があります。 FreeBSD 13.0 への SSH 接続では、Cisco SSH 互換の暗号、mac、および kex アルゴリズムのみがサポートされます。 『Release Notes for AsyncOS 15.0 for Cisco Secure Web Appliance』を参照してください。

関連項目

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

アプライアンス Web インターフェイスの使用

Web インターフェイスのブラウザ要件

Web インターフェイスにアクセスするための要件は次のとおりです。

- ブラウザで Cookie と JavaScript がサポートされ、有効になっている必要があります。
- また、ブラウザでは Cascading Style Sheet（CSS）を含む HTML ページをレンダリングできる必要があります。

- Cisco Secure Web Appliance は YUI（http://yuilibrary.com/yui/environments/）で設定されたターゲット環境に準拠しています。
- セッションは、非アクティブな状態が 30 分続くと自動的にタイムアウトします。
- Webインターフェイス内の一部のボタンとリンクを使用すると、さらにウィンドウが開きます。そのため、Webインターフェイスを使用するには、ブラウザのポップアップブロックを設定する必要があります。

（注） アプライアンスの設定を編集する場合は、一度に1つのブラウザウィンドウまたはタブを使用します。また、WebインターフェイスおよびCLIを同時に使用してアプライアンスを編集しないでください。複数の場所からアプライアンスを編集すると、予期しない動作が発生するので、サポートされません。

GUI にアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう設定されている必要があり、さらに、Cascading Style Sheet（CSS）を含む HTML ページを描画できる必要があります。

表 *2:* サポートされるブラウザおよびリリース

ブラウザ	Windows 10	MacOS 10.6
Safari	—	7.0 以降
Google Chrome	最新の安定バージョン	最新の安定バージョン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョン	最新の安定バージョン
Microsoft Edge	最新の安定バージョン	最新の安定バージョン

ブラウザは、そのブラウザの公式なサポート対象オペレーティング システムに対してのみサポートされます。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUI を使用するには、ブラウザのポップアップブロックの設定が必要な場合があります。

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス（AsyncOS 11.8 以降）でサポートされている解像度は、1280x800 ～ 1680x1050 です。サポートされるすべてのブラウザに対して最適に表示される解像度は 1440X900 です。

（注） シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

仮想アプライアンスでのWebインターフェイスへのアクセスのイネーブル化

デフォルトでは、HTTP および HTTPS インターフェイスは仮想アプライアンスで有効化されません。これらのプロトコルを有効にするには、コマンドラインインターフェイスを使用する必要があります。

ステップ 1 コマンドラインインターフェイスにアクセスします。コマンドラインインターフェイスへのアクセスを参照してください。

ステップ 2 `interfaceconfig` コマンドを実行します。

プロンプトで Enter を押すと、デフォルト値が受け入れられます。

HTTP および HTTPS のプロンプトを検索し、使用するプロトコルをイネーブルにします。

HTTP および HTTPS の AsyncOS API（モニターリング）のプロンプトを探し、使用するプロトコルをイネーブルにします。

アプライアンス Web インターフェイスへのアクセス

仮想アプライアンスを使用している場合は、仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化 （6 ページ） を参照してください。

ステップ 1 ブラウザを開き、 Secure Web Applianceの IP アドレス（またはホスト名）を入力します。アプライアンスが事前に設定されていない場合は、デフォルト設定を使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、`192.168.42.42` はデフォルト IP アドレス、`8080` は HTTP のデフォルトの管理ポートの設定、`8443` は `HTTPS` のデフォルトの管理ポートです。

アプライアンスが現在設定されている場合は、M1 ポートの IP アドレス（またはホスト名）を使用します。

（注） アプライアンスに接続するときはポート番号を使用する必要があります（デフォルトはポート 8080）。Web インターフェイスにアクセスするときにポート番号を指定しないと、デフォルトポート 80 になり、[ライセンスなしプロキシ（Proxy Unlicensed）] エラー ページが表示されます。

ステップ 2 （新しい Web インターフェイスのみ）レガシー Web インターフェイスにログインし、[Secure Web Appliance のデザインが新しくなりました。**お試しください!** リンクで新しい Web インターフェイスにアクセスできます。このリンクをクリックすると、Web ブラウザの新しいタブが開き、`https://wsa_appliance.com:<trailblazer-https-port>/ng-login` に移動します。ここで、`wsa_appliance.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

（注）
- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- 指定したアプライアンスのインターフェイスホスト名を DNS サーバーが解決できることを確認します。
- デフォルトでは、新しい Web インターフェイスでは、TCP ポート 6080、6443、および 4431 が動作可能である必要があります。これらのポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。
- 新しい Web インターフェイスにアクセスするためのデフォルト ポートは 4431 です。これは、`trailerblazerconfig` CLI コマンドを使用してカスタマイズできます。`trailblazerconfig` CLI コマンドの詳細については、Secure Web Appliance CLI コマンドを参照してください。
- 新しい Web インターフェイスでは、HTTP および HTTPS の AsyncOS API（モニタリング）ポートも必要です。デフォルトでは、これらのポートは 6080 および 6443 です。AsyncOS API（モニターリング）ポートは、`interfaceconfig` CLI コマンドでカスタマイズすることもできます。`interfaceconfig` CLI コマンドの詳細については、Secure Web Appliance CLI コマンドを参照してください。

  （注） ポートはデフォルトで有効になっていますが、これらのポートを無効にすると、アップグレード後に再び有効になります。

- これらのデフォルトポートを変更した場合は、新しい Web インターフェイスのカスタマイズされたポートもエンタープライズ ファイアウォールでブロックされないことを確認してください。

ステップ 3 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパスフレーズを入力します。

デフォルトで、アプライアンスには以下のユーザー名とパスフレーズが付属します。

- ユーザー名：**admin**
- パスフレーズ：**ironport**

admin のユーザー名でログインするのが初めての場合は、パスフレーズをすぐに変更するよう求められます。

ステップ 4 自分のユーザー名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）を表示するには、アプリケーション ウィンドウの右上の [ログイン（Logged in as）] エントリの前にある [最近のアクティビティ（recent-activity）] アイコン（成功は **i**、失敗は **!**）をクリックします。

Web インターフェイスでの変更内容のコミット

ステップ 1 [変更を確定（Commit Changes）] をクリックします。

ステップ 2 選択する場合、[コメント（Comment）] フィールドにコメントを入力します。

ステップ 3 [変更を確定（Commit Changes）] をクリックします。

（注） すべてをコミットする前に、複数の設定変更を行うことができます。

Web インターフェイスでの変更内容のクリア

ステップ 1 [変更を確定（Commit Changes）] をクリックします。

ステップ 2 [変更を破棄（Abandon Changes）] をクリックします。

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- ドイツ語
- 英語
- スペイン語
- フランス語
- イタリア語
- 日本語
- 韓国語
- ポルトガル語
- ロシア語
- 中国語
- 台湾語

Cisco SensorBase ネットワーク

Cisco SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネット トラフィックのグローバル ウォッチ リストを維持する脅威の管理データベースです。SensorBase は、既知のインターネット ドメインの信頼性の評価をシスコに提供します。Cisco Secure Web Appliance は、SensorBase データフィードを使用して、Web レピュテーションスコアを向上させます。

SensorBase の利点とプライバシー

Cisco SensorBase ネットワークへの参加は、シスコがデータを収集して、SensorBase 脅威管理データベースとそのデータを共有することを意味します。このデータには要求属性に関する情報およびアプライアンスが要求を処理する方法が含まれます。

シスコはプライバシーを維持する重要性を理解しており、ユーザー名やパスフレーズなどの個人情報または機密情報も収集または使用しません。また、ファイル名とホスト名に続く URL 属性は、機密性を保証するために難読化されます。復号化された HTTPS トランザクションでは、SensorBase ネットワークは IP アドレス、Web レピュテーション スコア、および証明書内のサーバー名の URL カテゴリのみを受信します。

SensorBase ネットワークへの参加に同意する場合、アプライアンスから送信されたデータは HTTPS を使用して安全に転送されます。データを共有すると、Web ベースの脅威に対応して、悪意のあるアクティビティから企業環境を保護するシスコの機能が向上します。

Cisco SensorBase ネットワークへの参加の有効化

（注） システムの設定時にデフォルトで [標準 SensorBase ネットワークに参加（Standard SensorBase Network Participation）] がイネーブルにされています。

ステップ 1 [セキュリティ サービス（Security Services）] > [SensorBase（SensorBase）] を選択します。

ステップ 2 [SensorBase ネットワークに参加（SensorBase Network Participation）] がイネーブルであることを確認します。

ディセーブルの場合、アプライアンスが収集するデータは SensorBase ネットワーク サーバーには戻されません。

ステップ 3 [加入レベル（Participation Level）] セクションで、以下のレベルのいずれかを選択します。

- **[制限（Limited）]。**基本的な参加はサーバー名情報をまとめ、SensorBase ネットワーク サーバーに MD5 ハッシュ パス セグメントを送信します。

- **[標準（Standard）]。**拡張された参加は、unobfuscatedパスセグメントを使用したURL全体をSensorBaseネットワーク サーバーに送信します。このオプションは、より強力なデータベースの提供を支援し、継続的に Web レピュテーション スコアの整合性を向上させます。

ステップ 4 [AnyConnectネットワークへの参加（AnyConnect Network Participation）] フィールドで、Cisco AnyConnect クライアントを使用して Cisco Secure Web Appliance に接続するクライアントから収集された情報を含めるかどうかを選択します。

AnyConnect クライアントは、Secure Mobility 機能を使用してアプライアンスに Web トラフィックを送信します。

ステップ 5 [除外されたドメインと IP アドレス（Excluded Domains and IP Addresses）] フィールドで、任意でドメインまたは IP アドレスを入力して、SensorBase サーバーに送信されたトラフィックを除外します。

ステップ 6 変更を送信し、保存します。

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。