製品およびリリースの概要

Web セキュリティ アプライアンスの概要

Cisco Web セキュリティ アプライアンスはインターネット トラフィックを代行受信してモニタし、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。

最新情報

Cisco AsyncOS 10.1.1 の新機能

このリリースには複数のバグ フィックスが含まれています。詳細については、『*Release Notes*』の「Fixed Issues」を参照してください。

Cisco AsyncOS 10.1.0 の新機能

機能	説明
アーカイブ検査	特定タイプの「検査可能なアーカイブ」を許可、ブロック、または検査できます。検査可能なアーカイブとは、WSA が展開して、そこに含まれる各ファイルを検査してファイル タイプ ブロック ポリシーを適用できるアーカイブ ファイルまたは圧縮ファイルのことです。検査可能なアーカイブのリストには、ZIP、Microsoft CAB、RAR、TAR などのアーカイブ タイプが含まれています。本ユーザ ガイドの「アクセス ポリシー：オブジェクトのブロッキング」を参照してください。
中央管理型アップグレード管理	この機能により、1 つのセキュリティ管理アプライアンス（SMA）を使用して複数の WSA を同時にアップグレードできます。各 WSA に異なるソフトウェア アップグレードを適用することもできます。
TCP ウィンドウの動的サイズ変更	CLI コマンド `networktuning` を使用すると、システムの負荷と使用可能なリソースに基づいて、TCP 送信/受信スペース バッファの動的サイズ変更を有効化/無効化できます。
TCP RST（リセット）転送の有効化/無効化	TCP RST（リセット）転送を有効または無効にするには、「`Do you want to forward TCP RST sent by server to client?`」オプションを CLI `advancedproxyconfig > MISCELLANEOUS` に追加できます。「Web セキュリティ アプライアンスの CLI コマンド」（B-6 ページ）を参照してください。
S600V のサポート	S600V 仮想アプライアンス モデルが OVF および KVM 導入でサポートされます。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。
ファイル レピュテーションとファイル分析のために、新しいヨーロッパ リージョン サーバが追加されました。	シスコでは、高度なマルウェア防御サービス用にヨーロッパ リージョンに 2 つの新しいサーバを追加しました。 ファイル レピュテーション サーバ：EUROPE（cloud-sa.eu.amp.cisco.com） ファイル分析サーバ：EUROPE（https://panacea.threatgrid.com） ファイル レピュテーションやファイル分析のために、これらのサーバを選択できます。本ユーザ ガイドの「ファイル レピュテーション フィルタリングとファイル分析」の章を参照してください。

Cisco AsyncOS 10.0.0 の新機能

機能	説明
curl コマンド	Web サーバに cURL 要求を直接またはプロキシ経由で送信します。返された要求や応答の HTTP ヘッダーから、Web ページをロードできなかった理由を判断できます。「Web セキュリティ アプライアンスの CLI コマンド」(B-6 ページ)を参照してください。 (注)　このコマンドは、TAC の監督のもとで管理者またはオペレータだけが使用できます。
参照元の例外	埋め込み/参照コンテンツ用に設定されたデフォルトのアクションに対する例外を定義できます。Web サイトでは、ソース ページとは分類が異なるコンテンツや、ソースとはタイプが異なるアプリケーションと見なされるコンテンツを埋め込んだり、参照することができます。デフォルトでは、ソース Web サイトの分類に関係なく、埋め込み/参照コンテンツは割り当てられたカテゴリまたはアプリケーションに選択したアクションに基づいてブロックまたはモニタされます。「埋め込み/参照コンテンツのブロックの例外」(9-12 ページ)を参照してください。
AMP プライベート クラウド	Cisco AMP 仮想プライベート クラウド アプライアンスを「エア ギャップ」モードでオンプレミス展開し、接続している WSA にプライベート ファイル レピュテーション フィルタリングを提供できるようになりました。「ファイル レピュテーションおよびファイル分析サービスの有効化と設定」(14-10 ページ)を参照してください。
AMP レポートの機能拡張	新しいレポート用パネルとディスプレイ、既存のレポート用パネルへのさらなる情報列の追加、特定のレポート間のクロスリンクなど、AMP 関連のレポート ページが拡張されました。 レトロスペクティブ アラートは、感染したファイル名や合計ユーザ数など、さらに情報を提供できるようになりました。また、レトロスペクティブ アラートのフォーマットもアップデートされ、より「読みやすく」なりました。 アクセス ログに新しいログ エントリ フィールドが追加されました。ログ エントリの末尾には次のようなファイル判定番号が付加されます。 1:不明 2:正常 3:悪意がある 4:スキャン不可
更新されたユーザ エージェントの一覧	ポリシーの定義時に選択できる使用可能なユーザ エージェントの一覧が更新され、拡張されました。この一覧は [詳細設定(Advanced)] > [ユーザ エージェントによるメンバーシップ(Membership by User Agent)] にあり、多数の機能ページ([識別プロファイル(Identification Profiles)]、[ルーティング ポリシー(Routing Policies)] など)からアクセスできます。

機能	説明
中間証明書	CLI コマンド advancedproxyconfig > HTTPS を使用して、「中間証明書の検出」を有効にできるようになりました。WSA は、中間証明書ストアを手動で検索してダウンロードする必要性をなくして、中間証明書の検証エラーを防ぐために、この検出プロセスを使用します。「Web セキュリティ アプライアンスの CLI コマンド」（B-6 ページ）を参照してください。
ライブ（サードパーティ）フィード	外部サーバからのデータ フィードに基づいてカスタム URL カテゴリを定義できます。これらのライブフィードのカスタム URL カテゴリは、ポリシー定義で使用できます。「カスタム URL カテゴリの作成と編集」（9-16 ページ）を参照してください。

このリリースには複数のバグ フィックスが含まれています。詳細については、『Release Notes』の「Fixed Issues」を参照してください。

関連項目

- 製品のリリース ノート：
  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には、ブラウザが JavaScript および Cookie をサポートし、受け入れがイネーブルになっている必要があります。また、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 Web セキュリティ アプライアンスは 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。

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。

手順 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（B-1 ページ）を参照してください。

手順 2　`interfaceconfig` コマンドを実行します。

プロンプトで Enter キーを押すと、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。

アプライアンス Web インターフェイスへのアクセス

はじめる前に

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（1-5 ページ）を参照してください。

手順 1　ブラウザを開き、Web セキュリティ アプライアンスの 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。

手順 2　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名とパスフレーズが付属します。

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

admin のユーザ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。

手順 3　自分のユーザ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の送信

（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。

手順 1　[変更を確定（Commit Changes）] ボタンをクリックします。

手順 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。

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

Web インターフェイスでの変更内容のクリア

手順 1　[変更を確定（Commit Changes）] ボタンをクリックします。

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

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。Web セキュリティ アプライアンスは、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イネーブル化

(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。

手順 1　[セキュリティ サービス（Security Services）] > [SensorBase] ページを選択します。

手順 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 サーバには戻されません。

手順 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名情報をまとめ、SensorBase ネットワーク サーバに 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。

手順 4　[AnyConnect ネットワークへの参加（AnyConnect Network Participation）] フィールドで、Cisco AnyConnect を使用して Web セキュリティ アプライアンス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。

手順 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 サーバに送信されたトラフィックを除外します。

手順 6　変更を送信し、保存します。