シスコASA FirePOWER モジュールの概要

シスコASA FirePOWER モジュール® は、Cisco ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、ASA5585-X-SSP-60 の各デバイスに展開できるモジュールです。モジュールは、ユーザの組織のセキュリティ ポリシー（ネットワークを保護するためのガイドライン）に準拠した方法でネットワーク トラフィックを処理するように設計されています。セキュリティ ポリシーにはアクセプタブル ユース ポリシー（AUP）も含まれていることがあります。AUP は、組織のシステムの使用方法に関するガイドラインを従業員に提供します。

このガイドでは、ASDM 経由でアクセス可能な、ASA FirePOWER モジュールの機能の onbox 設定に関する情報を提供します。各章の説明、図、および手順には、ユーザ インターフェイスをナビゲートする、システム パフォーマンスを最大にする、問題をトラブルシューティングする、といったことに役に立つ詳細な VMware 情報が記載されています。

注 ASA FirePOWER モジュールをホストしている ASA でコマンドの権限を有効にする場合は、特権レベル 15 を持つユーザ名でログインして、ASA FirePOWER のホーム、設定、およびモニタリングのページを参照できるようにする必要があります。読み取り専用、またはモニタリング専用の権限は、ステータス ページがサポートされている ASA FirePOWERのページにアクセスします。

以降のトピックでは、ASA FirePOWER モジュールの概要、主要なコンポーネント、およびこのマニュアルの使用方法について説明します。

ASA FirePOWER モジュールの概要

ASA FirePOWER モジュールは、ネットワーク セグメントにインストールされている ASA デバイスで動作し、分析用のトラフィックを監視します。

インラインで展開されたシステムは、*アクセス コントロール*を使用してトラフィックのフローに影響を与えることができ、これによって、ネットワークに出入りしたり通過するトラフィックを処理する方法を詳細に指定することができます。ネットワーク トラフィックについて収集したデータおよびそのデータから収集したすべての情報は、次に基づいてそのトラフィックをフィルタ処理および制御するために使用できます。

- シンプルで容易に決定されるトランスポート層およびネットワーク層の特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- 組織内の Microsoft Active Directory LDAP ユーザ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを得るのに最も有用である場合に行われます。たとえば、レピュテーション ベースのブラックリスト登録は、単純な送信元と宛先のデータを使用するため、プロセスの早期に禁止されたトラフィックをブロックできる一方で、侵入およびエクスプロイトの検出とブロックは最後の防衛ラインとなります。

ASA FirePOWERモジュール コンポーネント

以下のトピックでは、組織のセキュリティ、適用可能な使用ポリシー、およびトラフィック管理の戦略に対して有用な ASA FirePOWER モジュールの主な機能について説明します。

- アクセス コントロール（1-2 ページ）
- 侵入検知および防御（1-3 ページ）
- 高度なマルウェア防御とファイル制御（1-3 ページ）
- アプリケーション プログラミング インターフェイス（1-3 ページ）

アクセス コントロール

*アクセス制御*はポリシーベースの機能で、ユーザはこれを使用してネットワークを横断できるトラフィックを指定、検査、および記録することが可能です。*アクセス コントロール ポリシー*は、システムがネットワーク上のトラフィックを処理する方法を決定します。

最も単純なアクセス コントロール ポリシーは、その*デフォルト アクション*を使用してすべてのトラフィックを処理します。このデフォルト アクションは、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入についてトラフィックを検査するように設定することもできます。

より複雑なアクセス コントロール ポリシーはセキュリティ インテリジェンス データに基づいてトラフィックをブラックリスト登録することができ、また、*アクセス コントロール ルール*を使用してネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純にすることも複雑にすることもでき、複数の基準を使用してトラフィックを照合および検査します。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、ISE 属性、およびユーザ別にトラフィックを制御できます。高度なアクセス コントロール オプションには、復号化、前処理、およびパフォーマンスが含まれます。

各アクセス コントロール ルールには、一致するトラフィックをモニタするか、信頼するか、ブロックするか、許可するかを決定する*アクション*があります。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

侵入検知および防御

侵入検知および侵入防御は、トラフィックが宛先に許可される前のシステムの最後の防御ラインです。*侵入ポリシー*は、アクセス コントロール ポリシーによって呼び出される侵入検知および侵入防御の設定の定義済みセットです。*侵入ルール*およびその他の設定を使用して、これらのポリシーはセキュリティ違反がないかトラフィックを検査し、インライン展開では、悪意のあるトラフィックをブロックまたは変更できます。

システムによって提供されるポリシーが組織のセキュリティのニーズに完全に対応していない場合は、カスタム ポリシーを作成することで、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューを提供できます。設定できるカスタム ポリシーを作成および調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

高度なマルウェア防御とファイル制御

マルウェアの影響を特定して軽減しやすくするため、ASA FirePOWER モジュールのファイル制御、および高度なマルウェア対策の各コンポーネントによって、ネットワーク トラフィック内のファイル（マルウェア ファイル、アーカイブ ファイル内にネストされたファイルを含む）の伝送を検出、追跡、キャプチャ、分析、および必要に応じてブロックできます。

ファイル制御

*ファイル制御*により、デバイスは、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。ファイル制御は、全体的なアクセス制御設定の一部として設定します。アクセス制御ルールに関連付けられたファイル ポリシーによって、ルールの条件を満たすネットワーク トラフィックが検査されます。

ネットワークベースの高度なマルウェア防御（AMP）

ネットワークベースの*高度なマルウェア対策*（AMP）によって、複数のファイル タイプのマルウェアに関してネットワーク トラフィックを検査できます。

検出されたファイルは、保存済みかどうかに関係なく、ファイルの SHA-256 ハッシュ値を使用して単純な既知の性質の検索を行うためにCollective Security Intelligence クラウドに送信できます。このコンテキスト情報を使用して、特定のファイルをブロックまたは許可するようにシステムを設定できます。

マルウェア防御をアクセス制御設定全体の一部として設定することができます。アクセス制御ルールに関連付けられているファイル ポリシーは、ルールの条件に一致するネットワーク トラフィックを検査します。

アプリケーション プログラミング インターフェイス

アプリケーション プログラミング インターフェイス（API）を使用してシステムとやりとりするには、いくつかの方法があります。詳細については、次のいずれかのサポート サイトから追加資料をダウンロードできます。

- **シスコ：**（http://www.cisco.com/cisco/web/support/index.html）

ライセンスの規則

項の先頭に記載されているライセンス文は、この項に記載されている機能を使用するのに必要なライセンスを示しています。具体的なライセンスは次のとおりです。

Protection

Protectionライセンスでは、デバイスで侵入の検出および防御、ファイル制御、セキュリティインテリジェンスのフィルタリングを実行することができます。

Control

Controlライセンスでは、デバイスでユーザおよびアプリケーションの制御を実行することができます。Controlライセンスには Protection ライセンスが必要です。

URL フィルタリング

URL フィルタリングライセンスでは、デバイスが定期的に更新されるクラウドベースのカテゴリおよびレピュテーション データを使用して、モニタ対象ホストが要求した URL に基づいて、ネットワークを通貨できるトラフィックを判別できます。URL フィルタリングライセンスには Protection ライセンスが必要です。

マルウェア

マルウェアライセンスにより、デバイスはネットワークベースの高度なマルウェア防御（AMP）を実行できます。これはネットワーク上で転送されるファイルに含まれるマルウェアを検出し、ブロックする機能です。マルウェアライセンスには Protection ライセンスが必要です。

ライセンス付きの機能の多くは追加機能であるため、このドキュメントでは、各機能で最も必要なライセンスについてのみ記載しています。たとえば、ある機能で 、Protection、および Control のライセンスが必要な場合、Control のみが記載されています。ただし、機能が付加的でないライセンスを必要とする場合、マニュアルではそのライセンスをプラス（+）文字で示しています。

ライセンス文の「または」という語は、この項に記載されている機能を使用するには特定のライセンスが必要であるが、追加のライセンスで機能を追加することができることを示しています。たとえば、あるファイル ポリシーで、一部のファイル ルール アクションには Protectionライセンスが必要であり、その他のファイル ルール アクションではマルウェア ライセンスが必要であるとします。この場合、そのファイル ルールの説明のライセンス文には、「Protectionまたは マルウェア」と示されます。

IP アドレスの規則

IPv4 Classless Inter-Domain Routing（CIDR）の表記、および IPv6 の類似のプレフィックス長の表記を使用して、ASA FirePOWER モジュールの多数の個所におけるアドレス ブロックを定義することができます。

CIDR 表記では、ネットワーク IP アドレスとビット マスクの組み合わせを使用して、指定したアドレス ブロック内の IP アドレスを定義します。たとえば、次の表に CIDR 表記のプライベート IPv4 アドレス空間を示します。

表 1-1　CIDR 表記の構文例

CIDR ブロック	CIDR ブロックの IP アドレス	サブネットマスク	IP アドレスの数
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

同様に、IPv6 ではネットワーク IP アドレスとプレフィクス長の組み合わせを使用して、指定したブロック内の IP アドレスを定義します。たとえば、2001:db8::/32 は 32 ビットのプレフィクス長を持つ 2001:db8:: ネットワーク内の IPv6 アドレス（つまり、2001:db8:: から 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff まで）を指定します。

ASA FirePOWER モジュールでは、ユーザが CIDR またはプレフィクス長表記を使用して IP アドレスのブロックを指定すると、マスクまたはプレフィクス長によって指定されたネットワーク IP アドレス部分**のみ**が使用されます。たとえば、10.1.2.3/8 と入力した場合、ASA FirePOWER モジュールでは 10.0.0.0/8 が使用されます。

つまり、シスコでは CIDR またはプレフィクス長表記を使用するときにビット境界のネットワーク IP アドレスを使用する標準的な方法を推奨していますが、ASA FirePOWER モジュールではその必要はありません。