ファイアウォール機能

次のトピックでは、Secure Firewall Management Center またはクラウド提供の Firewall Management Center を使用して Secure Firewall Threat Defense で ASA ファイアウォール機能、または同等の機能を設定する方法について説明します。これらの機能は、『*CLI/ASDM Book 2: Cisco Secure Firewall ASA Series Firewall CLI/ASDM Configuration Guide*』ドキュメントに記載されている方法に基づいて大まかに編成されています。

アクセス コントロール

ASA CLI または ADSM を使用して ASA を設定する場合、常に一度に 1 つのデバイスを設定していることになります。

これに対して、Secure Firewall Management Center のアクセス コントロール ポリシーは常に共有ポリシーです。ポリシーを作成したら、1 つ以上のデバイスに割り当てます。

通常、複数のデバイスに対してアクセス コントロール ポリシーを作成します。たとえば、すべてのリモート ロケーション ファイアウォール（リモートサイトをメインの企業ネットワークに接続する）に同じポリシーを割り当てることができます。次に、コアデータセンターにあるファイアウォールに対して別のポリシーを設定することもできます。もちろん、デバイスごとに個別のポリシーを作成することもできますが、それは複数のデバイスマネージャを効率的に使用する方法ではありません。

特定のアクセスコントロールルールがデバイスに適用されるかどうかは、ルールで指定されたインターフェイスによって制御されます。

- インターフェイスを指定しない場合、ルールは、ポリシーが割り当てられているすべてのデバイスに適用されます。
- 特定のデバイスインターフェイスのリストであるオブジェクトであるセキュリティゾーンを指定した場合、ルールは、指定されたゾーンにインターフェイスを持つデバイスにのみ適用され、展開されます。セキュリティゾーンには、インターフェイス名だけでなく、

「デバイス上のインターフェイス」のペアも含まれます。たとえば、「inside on device1」は、「inside on device2」を含まないゾーンにある可能性があります。

次の表に、ASA の主なアクセスコントロール機能と、それらの機能または同等の機能を Secure Firewall Threat Defense デバイス上で設定する場所を示します。

表 *1*: アクセスコントロール機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールの**オブジェクト**	**オブジェクト** UI パス：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**。 「Object Management」を参照してください。 手順：動的オブジェクトを設定する	アクセス コントロール ポリシーを編集するときに、ネットワークおよびポート（サービス）オブジェクトを作成することもできます。 また、セキュリティグループタグと時間範囲もサポートされています。ネットワークサービスとローカルユーザーグループはサポートされていません（または必要ありません）。 アクセスコントロールルールで使用できる追加オブジェクト：アプリケーションフィルタ、地理位置情報、インターフェイス セキュリティ ゾーン、URL、およびVLANタグ。これらのオブジェクトは、ASA で使用できない機能に適用されます。
非アクセス コントロール グループ/ルールの**アクセスコントロールリスト（ACL）**。	**アクセス コントロール リスト（ACL）** UI パス：標準および拡張 ACL：**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**。 Ethertype ACL：**[デバイス（Devices）]** > **[FlexConfig]**。 「Object Management」および「FlexConfig Policies」を参照してください。 手順： • リモートアクセス（RA）VPN接続のトラフィックフィルタリングの設定：RA VPN 接続のトラフィックをフィルタリングするための拡張アクセスリストの作成、RA VPN 接続のトラフィックをフィルタリングするためのグループポリシーへの拡張アクセスリストの追加	標準または拡張 ACL のオブジェクトを作成し、ルーティングまたは ACL を必要とするその他の機能を設定するときにそれらのオブジェクトを使用します。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールルール：基本（ネットワーク、ポート、プロトコル、ICMP）。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」を参照してください。 手順： • デバイスのセットアップ：アクセスコントロールルールの追加 — 機能のウォークスルー、アクセス コントロール ポリシーの作成 • VTI トンネルの設定：VTI 経由の暗号化されたトラフィックを許可するアクセスコントロールルールの設定 • 新しいアクセス コントロール ポリシー UI：機能のウォークスルー – 新しい AC ポリシー UI へのアクセス、新しい AC ポリシー UI – ルールテーブル、新しい AC ポリシー UI – ルールの作成、新しい AC ポリシー UI – ルールの編集	アクセス コントロール ポリシーは、基本的な 5 タプルおよび VLAN アクセスコントロールルールをサポートします。さらに、地理位置情報オブジェクトを使用して、特定の地理的位置に関連付けられた IP アドレスをターゲットにすることができます。 プレフィルタポリシーを使用して、トンネルトラフィック（GRE など）やその他の 5 タプルトラフィックを制御することもできます。プレフィルタルールはアクセスコントロールルールの前に処理され、ASA では使用できません。**[ポリシー（Policies）]**>**[プレフィルタ（Prefilter）]**を参照してください。
アクセスコントロールルール：ユーザーベースの制御	**アクセス コントロール ルール** UI パス：ユーザー名とグループのマッピングを取得するためのルールを設定するには、**[ポリシー（Policies）]**>**[アイデンティティ（Identity）]**に移動します。 その後、アクセスコントロールルールでユーザー名とグループを選択できます。**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」および「User Identity Policies」を参照してください。 手順：動的オブジェクトのアクセス コントロール ポリシー ルールを設定する	ASA と比較して、ユーザー/グループ メンバーシップを取得するためのオプションは数多くあります。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
アクセスコントロールルール：セキュリティグループと Trustsec	**アクセス コントロール ルール** UI パス：Identity Services Engine を設定するには、**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[アイデンティティソース（Identity Sources）]**に移動します。 その後、アクセスコントロールルールでセキュリティグループタグを選択できます。**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」および「User Control with ISE/ISE-PIC」を参照してください。	Identity Services Engine を使用して、ユーザーベースの制御のためにユーザー名/ユーザーグループ情報を収集することもできます。
（ASA では使用できません。）アクセスコントロールルール：レイヤ 7 アプリケーション制御。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「Access Control Rules」を参照してください。	たとえば、同じプロトコルとポートを使用するアプリケーションのアクセスコントロールルールを記述して、さまざまなタイプの HTTP/HTTPS トラフィックを区別することができます。アプリケーションフィルタリングは、ASA で使用できるものよりも詳細な制御を適用するのに役立ちます。
アクセスコントロールルール：URL フィルタリング。	**アクセス コントロール ルール** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]**。 「URL Filtering」を参照してください。	URL カテゴリとレピュテーションに基づいてアクセスを制御するには、URL フィルタリングライセンスが必要です。 アクセス コントロール ポリシー内で定義されたセキュリティインテリジェンス ポリシーを使用して、URL またはネットワークオブジェクトに基づいて早期フィルタリングを行うこともできます。DNS ポリシーは、DNS ルックアップ要求に対して同じことを行うことができます。
デバイスへのトラフィックの **ICMP アクセスルール**（**icmp permit/deny** および **ipv6 icmp permit/deny** コマンド）。	**ICMP アクセスルール** UI パス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**、[ICMPアクセス（ICMP Access）] ページ。. 「Platform Settings」を参照してください。	アクセス コントロール ポリシーと同様に、プラットフォーム設定ポリシーは共有され、複数のデバイスにポリシーを適用できます。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
Cisco Umbrella	**Cisco Umbrella** UI パス：**[統合（Integration）] > [その他の統合（Other Integrations）] > [クラウドサービス（Cloud Services）]** **[ポリシー（Policies）] > [DNS]** **[デバイス（Devices）] > [VPN：サイト間（VPN: Site-to-Site）] > [SASE トポロジ（SASE Topology）]**。 「DNS Policies」および「Site-to-Site VPNs for Secure Firewall Threat Defense」を参照してください。	Cisco Umbrella DNS ポリシーと Cisco Umbrella SASE VPN トポロジを作成できます。

ネットワーク アドレス変換

アクセス コントロール ポリシーと同様に、ネットワークアドレス変換（NAT）ポリシーも共有されます。NAT ポリシーを作成してから、それを 1 つ以上のデバイスに割り当てます。FlexConfig ポリシーも共有されます。

特定の NAT ルールがデバイスに展開されるかどうかは、ルールをインターフェイスによって制限するか、すべてのインターフェイスにルールを適用するかによって異なります。

- インターフェイスを指定しない場合、ルールは、ポリシーが割り当てられているすべてのデバイスに適用されます。
- インターフェイス オブジェクトを指定すると、ルールは、指定されたオブジェクトにインターフェイスを持つデバイスにのみ適用され、展開されます。

次の表に、ASA の主なネットワークアドレス変換機能と、それらの機能または同等の機能を Secure Firewall Threat Defense デバイス上で設定する場所を示します。

表 *2:* ネットワークアドレス変換機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
ネットワークアドレス変換（**NAT**）：動的 NAT/PAT、静的 NAT、アイデンティティ NAT。	**ネットワーク アドレス変換（NAT）** UI パス：**[デバイス（Devices）]** > **[NAT]**。 「Network Address Translation (NAT)」を参照してください。 手順： • デバイスのセットアップ：NAT ポリシーの作成 — 機能のウォークスルー • 仮想ルーティングの設定：重複するアドレス空間によるインターネットアクセスの提供、仮想ルータの NAT の設定	オブジェクトと Twice NAT の両方を設定できます。ただし、それらは Secure Firewall Threat Defense では自動 NAT および手動 NAT と呼ばれます。
ポートブロック割り当てによるポートアドレス変換（**PAT**）。	**ポートブロック割り当てによるポートアドレス変換（PAT）。** UI パス：グローバル PAT ポートブロック割り当て設定（**xlate block-allocation** コマンド）を構成するには、**[デバイス（Devices）]** > **[FlexConfig]**を使用します。 次に、**[デバイス（Devices）]** > **[NAT]**を使用して PAT ルールを設定できます 「Network Address Translation (NAT)」および「FlexConfig Policies」を参照してください。	この機能は、キャリアグレードまたは大規模な PAT に使用されます。
Per-Session PAT または **Multi-Session PAT**（**xlate per-session** コマンド）。	**Per-Session PAT または Multi-Session PAT** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	Secure Firewall Threat Defense デフォルト設定には、ASA と同じ事前定義されたセッションごとのルールが含まれています。デフォルト以外の動作が必要な場合にのみ、構成が必要です。
アドレスとポートのマッピング（**MAP**）	**アドレスとポートのマッピング（MAP）** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	アドレスとポートのマッピング（MAP）は、IPv4 アドレスを IPv6 に変換するためのキャリアグレードの機能です。

アプリケーション インスペクション

Snort は Secure Firewall Threat Defense デバイスの主要検査エンジンです。ただし、ASA 検査は引き続き実行され、Snort 検査の前に適用されます。

Snort は多くの HTTP 検査を実行するため、ASA HTTP 検査エンジンはまったくサポートされておらず、設定できません。

多くの ASA 検査エンジンは、デフォルト設定によりデフォルトで有効になっています。ASA 検査エンジンが追加設定をサポートしている場合は、FlexConfig（共有ポリシー）を使用して設定を構成する必要があります。複数のデバイスに同じ設定を使用する場合、検査設定用に単一の FlexConfig ポリシーを作成し、該当するすべてのデバイスに適用できます。

単に検査をオフ（またはオン）にする必要がある場合は、FlexConfig の代わりに、各デバイスのデバイス CLI で **configure inspection** コマンドを使用できます。ただし、すべての可能なプロトコル検査がコマンドで使用できるわけではありません。

次の表に、さまざまな ASA 検査エンジンをリストし、Secure Firewall Threat Defense デバイスでデフォルトで有効になっているものを特定します。

表 *3:* アプリケーション インスペクション機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
基本インターネットプロトコルの**検査**	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。太字は、デフォルト設定で検査が有効になっていることを示します。 • DCERPC • **DNS** • **FTP** • **ICMP** • **ICMP エラー** • ILS • **IP オプション** • IPsec Pass Through • IPv6 • Lisp • **NetBIOS** • PPTP • **RSH** • SMTP/ESMTP • **SNMP** • **SQL*Net** • **Sun RPC** • **TFTP** • WAAS • XDMCP • VXLAN サポートされていません（Snort によって実行されます）：HTTP、IM（インスタントメッセージング）。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
音声とビデオのプロトコルの検査	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。太字は、デフォルト設定で検査が有効になっていることを示します。 • CTIQBE • **H.323 H.225** • **H.323 RAS** • MGCP • **rtsp** • **SIP モード（SIP** • **Skinny** • STUN
モバイルネットワークの検査	**(Inspection)]** UI パス：**[デバイス（Devices）]** > **[FlexConfig]**。 「FlexConfig Policies」を参照してください。	サポートされている検査は次のとおりです。これらの検査には、Carrier ライセンスが必要です。いずれもデフォルトでは有効になっていません。 • Diameter • GTP/GPRS • M3UA • SCTP • RADIUS アカウンティング（この検査には Carrier ライセンスは必要ありません）

サービスポリシー、接続設定、脅威検出

次の表に、デバイスを通過する接続のいくつかの側面を制御する、大まかに関連する機能をいくつか示します。これらの設定のほとんどには、ほとんどの場合に機能するデフォルトがあります。

表 *4:* サービス ポリシー、接続設定、脅威検出機能

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
グローバル タイムアウト	**グローバル タイムアウト** UI パス：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**、[タイムアウト（Timeouts）] ページ。 「Platform Settings」を参照してください。	プラットフォーム設定は共有ポリシーです。これらの設定は、ポリシーが割り当てられた各デバイスに適用されます。
接続設定の**サービスポリシー**	**Threat Defense サービス ポリシー** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択してから、ポリシーの編集中に [詳細設定（Advanced Settings）] で [脅威防御サービスポリシー（Threat Defense Service Policy）] を見つけます。 「Service Policies」を参照してください。	これらの設定には、TCP ステートバイパス、TCP シーケンスランダム化、TCP インターセプト、デッド接続検出（DCD）、TCP 正規化、およびトラフィッククラスごとの一般的な接続制限とタイムアウトが含まれます。 脅威防御サービスポリシーは、アクセス コントロール ポリシーの一部として定義されます。これは、1 つ以上のデバイスに割り当てる共有ポリシーです。 特定のインターフェイスに制限するルールは、そのインターフェイスを含むデバイスでのみ構成されます。グローバルルールは、アクセス コントロール ポリシーに割り当てられたすべてのデバイスに適用されます。
Quality of Service（QoS）	**Quality of Service（QoS）** UI パス：**[デバイス（Devices）]** > **[QoS]**。 「Quality of Service」を参照してください。	QoS ポリシーは共有されますが、ポリシーの各ルールは 1 つ以上のインターフェイスを指定する必要があります。ルールにデバイス上のインターフェイスが含まれている場合にのみ、ルールはデバイスに構成されます。
脅威検出（threat-detection コマンド）。	**脅威の検出** UI パス：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** を選択してから、ポリシーの編集中に [詳細設定（Advanced Settings）] で [脅威検出（Threat Detection）] を見つけます。 「Threat Detection」を参照してください。	Secure Firewall Threat Defense 機能は、ASA 機能と完全に重複するものではありませんが、新しい機能が含まれています。FlexConfig を使用して、ASA コマンドバージョンを展開することもできます。

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。