Cisco Secure Firewall ASA の概要

Cisco Secure Firewall ASA は、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール オペレーション、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.23(1) の新機能

リリース：**2025 年 3 月 5 日**

特長	説明
プラットフォーム機能	
Cisco Secure Firewall 1230/1240/1250	Cisco Secure Firewall 1230/1240/1250 は、1RU ラックマウント可能なファイアウォールです。
Cisco Secure Firewall 4200 の接続制限の引き上げ	最大接続数が引き上げられました。 • 4225：3,000 万 → **9,000 万** • 4245：6,000 万 → **18,000 万**
ファイアウォール機能	
RADIUS Message-Authenticator 属性のサポート。	Message-Authenticator 属性は、Blast- RADIUS 攻撃を防ぐために使用されます。メッセージオーセンティケータをサポートするようにRADIUSサーバーをアップグレードした場合は、このオプションを有効にして、Blast- RADIUS攻撃を防御できます。有効にする場合、すべての要求と応答にメッセージオーセンティケータが含まれている必要があります。含まれていない場合、認証は失敗します。 **message-authenticator-required** コマンドが追加されました。
新規 Umbrella API。	秘密キーを持つ API キーを使用する Cisco Umbrella オープンAPIを使用して、Cisco Umbrella を設定できるようになりました。 次のコマンドが追加されました。 **token-request-credential**
フロー オフロードは Secure Firewall 3100/4200 に対してデフォルトで有効です	フロー オフロードはデフォルトで有効です。 追加/変更されたコマンド： **flow-offload enable**
高可用性とスケーラビリティの各機能	

特長	説明
すべての Cisco Secure Firewall 1200 モデルでマルチ コンテキストをサポート	マルチ コンテキスト モードのサポートが追加されました。Cisco Secure Firewall 1210/1220 • Cisco Secure Firewall 1210CE-5 コンテキスト。 • Cisco Secure Firewall 1210CP：5 コンテキスト。 • Cisco Secure Firewall 1220CX：10 コンテキスト。 スイッチポートはマルチ コンテキスト モードではサポートされていません。マルチ コンテキスト モードに変換する前に、すべてのインターフェイスをルータ インターフェイスに変換する必要があります。 Cisco Secure Firewall 1230/1240/1250 も最初のリリースでマルチ コンテキスト モードをサポートしています。 • Cisco Secure Firewall 1230：25 コンテキスト。 • Cisco Secure Firewall 1240：25 コンテキスト。 • Cisco Secure Firewall 1250：25 コンテキスト。
クラスタ リダイレクト： Cisco Secure Firewall 4200 非対称クラスタ トラフィックのフロー オフロードのサポート	非対称フローの場合、クラスタリダイレクトにより、転送ノードはハードウェアにフローをオフロードできます。この機能はデフォルトで有効になっています。 既存のフローのトラフィックが別のノードに送信されると、そのトラフィックはクラスタ制御リンクを介してオーナー ノードにリダイレクトされます。非対称フローは、クラスタ制御リンクに大量のトラフィックを作成する可能性があるため、フォワーダにこれらのフローをオフロードさせると、パフォーマンスが向上します。 追加/変更されたコマンド：**flow-offload cluster-redirect**、**show conn**、**show flow-offload flow**, , **show flow-offload flow protocol**、**show flow-offload info**。
フェールオーバー中のロールスイッチ時間の短縮	フェールオーバーが発生すると、新しいアクティブデバイスが MAC アドレスエントリごとにマルチキャストパケットを生成して、すべてのブリッジ グループ インターフェイスに送信し、アップストリームスイッチにルーティングテーブルを更新させます。マルチキャストパケットを生成してブリッジインターフェイスに送信するこのタスクは、データプレーンで非同期に実行されるようになったため、コントロールプレーンでの重要なフェールオーバータスクを遅延なく続行できます。 この機能拡張により、フェールオーバー中のロールスイッチ時間が短縮され、ダウンタイムが短縮されます。
クラスタノード参加時の MTU ping テスト	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
インターフェイス機能	

特長	説明
Cisco Secure Firewall 1210CP IEEE 802.3bt のサポート（PoE++ および Hi-PoE）	IEEE 802.3bt のサポートに関連する次の改善を確認してください。 • PoE++ と Hi-PoE：ポートあたり最大 90 W。 • シングルシグネチャおよびデュアルシグネチャの受電デバイス（PD）。 • パワーバジェットが先着順で行われます。 • **show power inline** にパワーバジェットフィールドが追加されました。 新規/変更されたコマンド：**power inline**、**show power inline**
ライセンス機能	
ASA 仮想に対する柔軟な永続ライセンスの予約	ASA 仮想の場合、RAM と vCPU に関係なく、モデル固有のライセンスを永続ライセンス予約用に設定できます。ASA 仮想に割り当てられたメモリに関係なく、永続ライセンスの予約ライセンスを切り替えることができます。また、モデルライセンスを変更せずに、 ASA 仮想 に割り当てられたメモリと vCPU を変更することもできます。 ASA 仮想 の 9.23.1 より前のバージョンにダウングレードすると、ライセンスのステータスが [未登録（Unregistered）] になります。柔軟な永続ライセンス予約で ASA 仮想 をダウングレードしないことをお勧めします。 次のコマンドが追加されました。 **license smart flex-model**
管理、モニタリング、およびトラブルシューティングの機能	
TLS デバイス証明書に対する Automated Certificate Management Environment（ACME）プロトコル	ASA トラストポイントに自動証明書管理環境（ACME）プロトコルを設定して、TLS デバイス証明書を管理できます。ACME は、自動更新、ドメイン検証、および簡単な登録と失効によって、簡素化された証明書管理を可能にします。認証に Let's Encrypt CA サーバーを使用するか、他の ACME サーバーを使用するかを選択できます。ACME は認証に http01 方式を使用します。 変更されたコマンド **crypto ca trustpoint enrollment protocol crypto ca authenticate**
VPN 機能	
Secure Firewall 4200 のクラスタリングを使用した分散型サイト間 VPN	Firepower 4200 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ノードだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn-mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show conn detail**、**show crypto ikev2 stats**

特長	説明
分散型サイト間 VPN モードの Cisco Secure Firewall 4200 のクラスタ制御リンクのトラフィックの IPsec フローのオフロード	分散型サイト間 VPN モードの非対称フローの場合、IPsec フロー オフロードにより、フローオーナーは、クラスタ制御リンクを介して転送されたハードウェア内の IPsec トラフィックを復号できます。この機能は構成可能ではありません。IPsec フローのオフロードを有効にすると常に使用できます。 追加/変更されたコマンド： **flow-offload-ipsec**、**show crypto ipsec sa detail**

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザーによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザー ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバーまたは FTP サーバーなど、外部のユーザーが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによってDMZに許可されるアクセスは限定されますが、DMZにあるのは公開サーバーだけのため、この地帯が攻撃されても影響を受けるのは公開サーバーに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバーと協調するといった手段によって、内部ユーザーが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザーに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数のDMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

アクセス ルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループ インターフェイスでは、EtherType アクセス ルールを適用して、非 IP トラフィックを許可できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は、IP グラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバーへの発信アクセスを禁止できますが、このような方法でWebサイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定できます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoSとは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャニング脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- Transparent

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えな

いようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherTypeアクセスリストを使用するマルチキャストストリームが許可されます。

ルーテッドモードでブリッジグループの設定、およびブリッジグループと通常インターフェイスの間のルートの設定を行えるように、ルーテッドモードではIntegrated Routing and Bridgingをサポートしてます。ルーテッドモードでは、トランスペアレントモードの機能を複製できます。マルチコンテキストモードまたはクラスタリングが必要ではない場合、代わりにルーテッドモードを使用することを検討してください。

ステートフル インスペクションの概要

ASAを通過するトラフィックはすべて、アダプティブセキュリティアルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケットフィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケットシーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCPステートバイパス機能を使用すると、パケットフローをカスタマイズできます。

ただし、ASAのようなステートフルファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASAは、パケットをアクセスリストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロールプレーンパス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセスリストとの照合チェック
  - ルートルックアップ
  - NAT変換（xlates）の割り当て
  - 「ファストパス」でのセッションの確立

  ASAは、TCPトラフィックのファストパスに転送フローとリバースフローを作成します。ASAは、高速パスも使用できるように、UDP、ICMP（ICMPインスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファストパスを使用できます。

（注） SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ7インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換
  - レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

  レイヤ7インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

  確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパ

ケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザーの認証
- ユーザー アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ユニット上でのみ実行します。コンフィギュレーションは、メンバーユニットに複製されます。

特殊なサービスおよびレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンライン ヘルプとは別の場所にあります。

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバーのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティ アプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『Cisco ASA Botnet Traffic Filter Guide』
- 『Cisco ASA NetFlow Implementation Guide』
- 『Cisco ASA Unified Communications Guide』
- 『Cisco ASA WCCP Traffic Redirection Guide』
- 『SNMP Version 3 Tools Implementation Guide』

レガシー サービス ガイド

レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則

- IP スプーフィングの防止などの保護ツールの使用（**ip verify reverse-path**）、フラグメント サイズの設定（**fragment**）、不要な接続のブロック（**shun**）、TCP オプションの設定（ASDM 用）、および基本 IPS をサポートする IP 監査の設定（**ip audit**）。
- フィルタリング サービスの設定

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。