セキュリティ機能の概要

セキュリティ機能の概要

スイッチは、スイッチ ハードウェアによって、限定されたフィーチャ セットを持つ LAN Base イメージまたは LAN Lite イメージをサポートします。 セキュリティ機能は次のとおりです。

- FIPS 認定

  Catalyst 2960-X スイッチに搭載された Cisco IOS Release 15.0(2)XE は、FIPS 140-2 の認証を受け、Common Criteria および米国政府ネットワーク デバイス セキュリティ要件に準拠しています。

  FIPS 140-2 は、暗号化に焦点を当てた認証であり、多くの政府およびエンタープライズの顧客により義務付けられています。これは、スイッチで実行される暗号化および復号化処理が、これらの処理を保護するために、承認された FIPS 暗号化強度および管理方法に準拠していることを保証します。

- IPv6 ファースト ホップ セキュリティ：IPv6 ネットワークの持つ脆弱性から保護するためにファースト ホップ スイッチに適用されるセキュリティ機能のセット。 これらには、バインディング統合ガード（バインディング テーブル）、ルータ アドバタイズメント ガード（RA ガード）、DHCP ガード、IPv6 ネイバー探索検査（ND ガード）などがあります。

- Web 認証：Web ブラウザを使用して認証する IEEE 802.1x 機能をサポートしないサプリカント（クライアント）を許可します。

  （注） Web 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- ローカル Web 認証バナー：Web 認証ログイン画面に表示されるカスタム バナーまたはイメージ ファイル。

- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。

（注） Web 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へのパスワード保護付きアクセス（読み取り専用および読み書きアクセス）。不正な設定変更を防止します。
- セキュリティ レベル、通知、および対応するアクションを選択できる、マルチレベル セキュリティ。
- セキュリティを確保できるスタティック MAC アドレッシング。
- 保護ポート オプション。同一スイッチ上の指定ポートへのトラフィック転送を制限します。
- ポートにアクセスできるステーションの MAC アドレスを制限または特定するポート セキュリティ オプション。
- 違反発生時に、ポート全体をシャットダウンするのではなく、そのポートの VLAN をシャットダウンする VLAN 対応ポート セキュリティ オプション。
- ポート セキュリティ エージング。ポートのセキュア アドレスにエージング タイムを設定します。
- 指定した入力割合を超えたパケットをドロップして、スイッチへの着信プロトコル トラフィックの割合を制御する、プロトコル ストーム プロテクション。
- BPDU ガード。無効なコンフィギュレーションが発生した場合に、PortFast が設定されているポートをシャットダウンします。
- 標準および拡張 IP アクセス コントロール リスト（ACL）は、レイヤ 2 インターフェイス（ポート ACL）でのインバウンドなセキュリティ ポリシーを定義します。
- MAC 拡張アクセス コントロール リスト。レイヤ 2 インターフェイスの着信方向のセキュリティ ポリシーを定義します。
- 非 IP トラフィックをフィルタリングする、送信元および宛先 MAC ベースの ACL。
- 信頼できないホストと DHCP サーバの間の信頼できない DHCP メッセージをフィルタリングする DHCP スヌーピング。
- DHCP スヌーピング データベース、および IP ソース バインディングに基づいてトラフィックをフィルタリングすることにより、非ルーテッド インターフェイスでのトラフィックを制限する IP ソース ガード。
- 不正な ARP 要求や応答を同じ VLAN 上のその他のポートにリレーしないことにより、スイッチに対する悪意のある攻撃を回避するためのダイナミック ARP インスペクション。
- IEEE 802.1x ポートベース認証。不正なデバイス（クライアント）によるネットワーク アクセスを防止します。 次の 802.1x 機能がサポートされます。

- データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポートにおいて、単独で認証できるようにするマルチドメイン認証（MDA）。

（注） MDA を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- MDA のダイナミック音声 VLAN（仮想 LAN）。ダイナミック音声 VLAN が MDA 対応ポートで可能になります。
- VLAN 割り当て。802.1x 認証ユーザを特定の VLAN に制限します。
- マルチ認証モードで設定されたポートでの VLAN 割り当てのサポート。 RADIUS サーバは、ポートで最初に認証されるホストに VLAN を割り当て、後続のホストは同じ VLAN を使用します。 音声 VLAN 割り当ては、1 つの IP フォンに対してサポートされます。

（注） この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- ポート セキュリティ。802.1x ポートへのアクセスを制御します。
- 音声 VLAN。ポートが許可ステートか無許可ステートかにかかわらず、Cisco IP Phone の音声 VLAN へのアクセスを許可します。
- IP Phone 検出機能拡張。Cisco IP Phone を検出し識別します。
- ゲスト VLAN。802.1x に適合しないユーザに限定的なサービスを提供します。
- 制限付き VLAN。802.1x に準拠はしているが、標準の 802.1x で認証するためのクレデンシャルを持っていないユーザに制限付きのサービスを提供します。

（注） 制限付き VLAN で認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 802.1x アカウンティング。ネットワーク使用をトラッキングします。
- 802.1x と LAN の Wake-on-LAN（WoL）機能。休止状態の PC に、特定のイーサネット フレームを送信して起動させます。
- 802.1x 準備状態チェック。スイッチで IEEE 802.1x を設定する前に、接続されたエンドホストの準備状態を判断します。

（注） 802.1x 準備状態チェックを使用するには、スイッチが LAN Base イメージを実行している必要があります。

- セキュリティ違反が発生した VLAN だけでトラフィック違反アクションを適用するための音声認識 802.1x セキュリティ。

（注） 音声認識 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- MAC 認証バイパス（MAB）。クライアント MAC アドレスに基づいてクライアントを許可します。

（注） MAC 認証バイパスを使用するには、スイッチが LAN Base イメージを実行している必要があります。

- デバイスのネットワーク アクセスを許可する前の、エンドポイント システムやクライアントのウイルス対策の状態またはポスチャに関する Network Admission Control（NAC）レイヤ 2 802.1x 検証。

（注） NAC を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 802.1X スイッチ サプリカントを持つ Network Edge Access Topology（NEAT）、CISP を使ったホスト認証、および自動イネーブル化。これらにより、別のスイッチへのサプリカントとして、配線クローゼットの外のスイッチが認証されます。
- 認証される前にネットワークへのアクセスをホストに許可するための、オープンアクセスを使用した IEEE 802.1x。
- ダウンロード可能な ACL とリダイレクト URL を使用した IEEE 802.1x 認証。Cisco Secure ACS サーバから認証されたスイッチへのユーザ単位の ACL ダウンロードを使用できるようになります。
- スタティック ACL が設定されていないポートでの認証デフォルト ACL のダイナミックな作成または接続のサポート。

（注） この機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 新しいホストを認証するときに、ポートが思考する認証メソッドの順序を設定するための柔軟な認証シーケンス。
- マルチユーザ認証。複数のホストが、802.1x 対応ポートを認証できるようになります。

- TACACS+。IPv4 および IPv6 対応の TACACS サーバを介してネットワーク セキュリティを管理する独自の機能。
- IPv4 および IPv6 対応の認証、許可、アカウンティング（AAA）サービスを使用して、リモートユーザの ID の検証、アクセスの許可、アクションの追跡を実行するための RADIUS。
- IPv6 上での機能向けに、RADIUS、TACACS+、および SSH を拡張。
- HTTP 1.1 サーバ認証、暗号化、メッセージ整合性、HTTP クライアント認証用に Secure Socket Layer（SSL）バージョン 3.0 がサポートされ、安全な HTTP 通信が可能になります（ソフトウェアの暗号化バージョンが必要）。
- ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。
- スタティック ホストでの IP ソース ガードのサポート。
- RADIUS 認証の変更（CoA）。特定のセッション認証された後で、その属性を変更します。AAA でユーザ、またはユーザ グループのポリシーに変更がある場合、管理者は Cisco Identity Services Engine または Cisco Secure ACS などの AAA サーバから、RADIUS CoA パケットを送信し、新しいポリシーに適用することができます。
- IEEE 802.1x ユーザ ディストリビューション。さまざまな VLAN にわたってユーザをロードバランシングすることにより、（ユーザ グループに対して）複数の VLAN を使った配置で、ネットワークのスケーラビリティを向上させることができます。 認証されたユーザは、RADIUS サーバにより割り当てられた、グループ内で最も空いている VLAN に割り当てられます。
- マルチ ホスト認証を使った、重要な VLAN のサポート。これにより、ポートがマルチ認証用に設定され、AAA サーバが到達不能になった場合でも、重要なリソースへのアクセスができるように、このポートが重要な VLAN に配置されます。
- ポート ホスト モードを変更し、オーセンティケータのスイッチ ポートに標準ポート設定を適用するために Network Edge Access Topology（NEAT）をサポート。
- VLAN-ID ベースの MAC 認証。ユーザ認証のために VLAN と MAC のアドレス情報を結合して、許可されていない VLAN からのネットワーク アクセスを阻止します。
- MAC 移動。モビリティのイネーブル化を制約することなく、ホスト（IP フォンの背後で接続されたホストを含む）が同じスイッチ内のポート間を移動できるようになります。 MAC 移動では、もう 1 つのポートに同じ MAC アドレスが再登場した場合、スイッチはこれをまったく新しい MAC アドレスと同様に扱います。
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）を使った 3DES および AES のサポート。 このリリースでは、168 ビット Triple Data Encryption Standard（3DES）と、SNMPv3 への 128 ビット、192 ビット、および 256 ビットの Advanced Encryption Standard（AES）暗号化アルゴリズムに対するサポートが追加されます。

- Cisco TrustSec SXP プロトコルのサポート。