エンドポイントアドミッションコントロールの設定

このモジュールでは、TrustSecネットワークでの認証および許可のためのエンドポイントアドミッション コントロール（EAC）のアクセス方式について説明します。

- エンドポイント アドミッション コントロールの概要 （1 ページ）
- 例：Example: 802.1X 認証の設定 （2 ページ）
- 例：MAC 認証バイパスの設定 （2 ページ）
- 例：Web 認証プロキシの設定 （2 ページ）
- 例：Flexible Authentication（FlexAuth; フレキシブル認証）シーケンスおよびフェールオーバー コンフィギュレーション （3 ページ）
- 802.1X ホスト モード （3 ページ）
- 認証前オープン アクセス （4 ページ）
- 例：DHCP スヌーピングおよび SGT の割り当て （4 ページ）
- エンドポイント アドミッション コントロールの機能履歴 （4 ページ）

エンドポイント アドミッション コントロールの概要

TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。TrustSec エンドポイント認証では、TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイス トラッキングによってアクセス デバイスでセキュリティ グループ タグ（SGT）に関連付けられます。アクセスデバイスは、継続的に更新される送信元 IP と SGT のバインディングテーブルを維持する TrustSec ハードウェア対応出力のデバイスに、SXP 経由でそのアソシエーション（バインド）を送信します。パケットは、セキュリティグループ ACLS（SGACL）を適用することにより、TrustSec ハードウェア対応デバイスによって出力でフィルタリングされます。

認証および許可のためのエンドポイント アドミッション コントロール（EAC）アクセス方式には、次のものがあります。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）

- Web 認証（WebAuth）

すべてのポートベース認証は、authentication コマンドでイネーブルにできます。各アクセス方式はポート単位で個別に設定する必要があります。複数の認証モードが設定され、アクティブ方式が失敗すると柔軟な認証シーケンスおよびフェールオーバー機能により管理者は、フェールオーバーおよびフォールバック シーケンスを指定することができます。802.1X ホスト モードは、802.1X ポートごとに接続できるエンドポイントのホスト数を決定します。

例：Example: 802.1X 認証の設定

次に、ギガビット イーサネット ポートでの基本的な 802.1x の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x system-auth-control
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
```

例：MAC 認証バイパスの設定

MAC 認証バイパス（MAB）は 802.1X 対応ではないホストまたはクライアントが 802.1X をイネーブルにしたネットワークに参加できるようにします。MAB をイネーブルにする前に、802.1X 認証をイネーブルにする必要はありません。

次の例では、基本的な MAB 設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# mab
```

MAB 認証の設定の詳細については、アクセスデバイスのコンフィギュレーション ガイドを参照してください。

例：Web 認証プロキシの設定

Web 認証プロキシ（WebAuth）は、ユーザーが Web ブラウザを使用して、アクセス デバイスの Cisco IOS Web サーバー経由で Cisco Secure ACS にログイン クレデンシャルを送信できるようにするものです。WebAuth は独立してイネーブルにできます。これは、802.1X または MAB の設定は必要ではありません。

次の例では、ギガビット イーサネット ポートでの基本的な WebAuth 設定の例を示します。

```
Device(config)# ip http server
Device(config)# ip access-list extended POLICY
Device(config-ext-nacl)# permit udp any any eq bootps
Device(config-ext-nacl)# permit udp any any eq domain
Device(config)# ip admission name HTTP proxy http
Device(config)# fallback profile FALLBACK_PROFILE
Device(config-fallback-profile)# ip access-group POLICY in
Device(config-fallback-profile)# ip admission HTTP
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group
POLICY in
```

例：Flexible Authentication（FlexAuth; フレキシブル認証）シーケンスおよびフェールオーバー コンフィギュレーション

Flexible Authentication（FlexAuth; フレキシブル認証）シーケンス（FAS）を使用すると、802.1X、MAB、および WebAuth 認証方式用にアクセスポートを設定でき、1 つ以上の認証方式が使用できない場合にフォールバックシーケンスを指定できます。デフォルトのフェールオーバーシーケンスは次のとおりです。

- 802.1X ポートベースの認証
- MAC 認証バイパス
- Web 認証

レイヤ 2 認証はレイヤ 3 の認証前に常に実行されます。つまり、802.1X と MAB は WebAuth の前に発生する必要があります。

次の例では、MAB、dot1X および WebAuth の順で認証シーケンスを指定します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 2/1
Device(config-if)# authentication order mab dot1x webauth
Device(config-if)# ^Z
```

FAS の詳細については、『Flexible Authentication Order, Priority, and Failed Authentication』を参照してください。

802.1X ホスト モード

ポート単位で 4 種類の分類モードを設定できます。

- Single Host：1 個の MAC アドレスを持つインターフェイス ベースのセッション

- Multi Host：ポートごとに複数の MAC アドレスを持つインターフェイス ベースのセッション
- Multi Domain：MAC + ドメイン（VLAN）セッション
- Multi Auth：ポートごとに複数の MAC アドレスを持つ MAC ベースのセッション

認証前オープン アクセス

認証前オープンアクセス機能は、ポートの認証の実行前に、クライアントとデバイスがネットワーク アクセスを取得できるようにするものです。このプロセスが主に、PXE がタイムアウトする前にデバイスがネットワークにアクセスし、サプリカントが含まれる可能性のあるブート可能イメージをダウンロードする必要がある PXE のブートのシナリオで必要です。

例：DHCP スヌーピングおよび SGT の割り当て

認証プロセス後は、デバイス認証が発生します（たとえば、ダイナミック VLAN 割り当て、ACL プログラミングなど）。TrustSec ネットワークの場合、セキュリティ グループ タグ（SGT）は Cisco ACS のユーザー コンフィギュレーションごとに割り当てられます。SGT はそのエンドポイントから DHCP スヌーピングおよび IP デバイス トラッキング インフラストラクチャを使用して送信されたトラフィックにバインドされます。

次の例では、アクセスデバイスで DHCP スヌーピングおよび IP デバイストラッキングを有効にします。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10
Device(config)# no ip dhcp snooping information option
Device(config)# ip device tracking
```

エンドポイントアドミッションコントロールの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	エンドポイントアドミッション コントロール	Cisco TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。Cisco TrustSec エンドポイント認証では、Cisco TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイストラッキングによってアクセスデバイスで SGT に関連付けられます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。