200/220/300シリーズスイッチでの802.1Xホストおよびセッション認証の設定

目的

802.1Xは、ポートに接続されているデバイスに認証方式を提供する、ポートベースのネットワークアクセス制御(PNAC)のIEEE標準です。スイッチの管理GUIの[Host and Session Authentication]ページを使用して、ポート単位で使用する認証タイプを定義します。ポート単位の認証は、ネットワーク管理者が必要な認証タイプに基づいてスイッチポートを分割できるようにする機能です。[Authenticated Hosts]ページには、認証されたホストに関する情報が表示されます。

この記事では、ポート単位でホスト認証とセッション認証を設定する方法、および200/220/300シリーズマネージドスイッチの802.1Xセキュリティ設定で認証済みホストを表示する方法について説明します。

該当するデバイス

- Sx200シリーズ
- Sx220シリーズ
- Sx300シリーズ

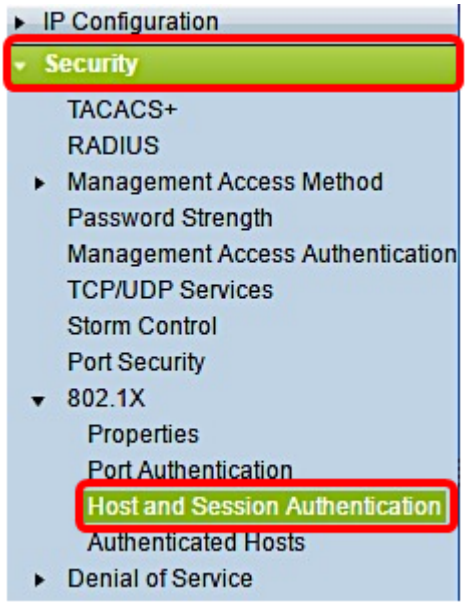
[Software Version]

- 1.4.5.02 — Sx200シリーズ、Sx300シリーズ
- 1.1.0.14 — Sx220シリーズ

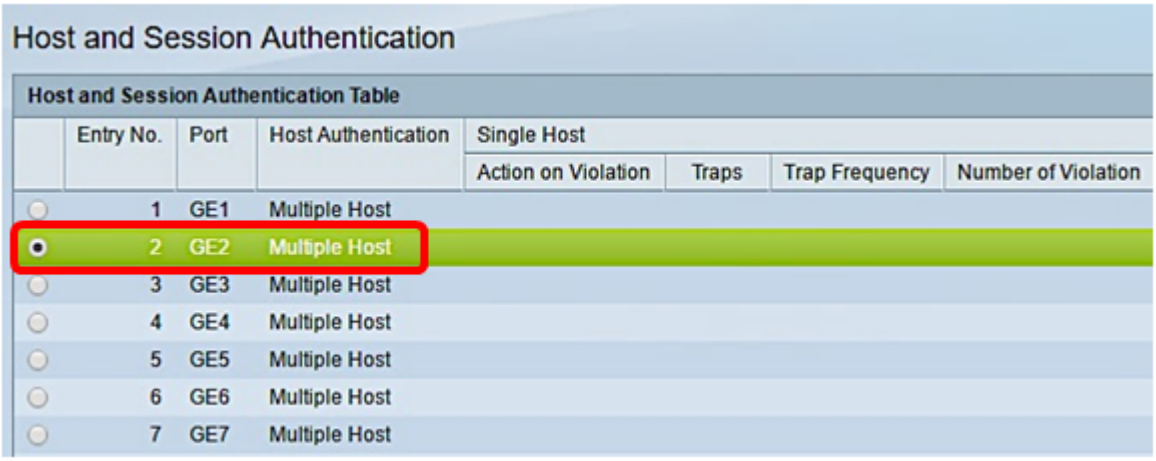
ホストおよびセッションの認証

ステップ 1：Webベースのユーティリティにログインし、[Security] > [802.1X] > [Host and Session Authentication] を選択します。

注：次のイメージは、SG220-26Pスマートスイッチから取得したものです。

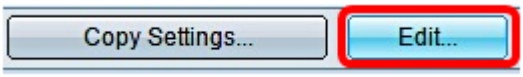


ステップ 2：編集するポートのオプションボタンをクリックします。

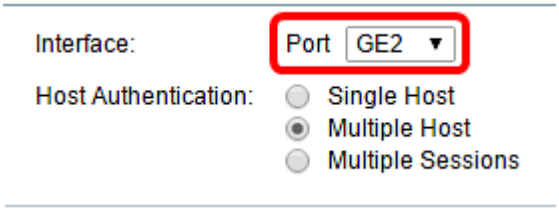


注：この例では、ポートGE2が選択されています。

ステップ 3：**Edit**をクリックして、指定したポートのホストおよびセッションの認証を編集します。



ステップ 4：[Edit Port Authentication]ウィンドウがポップアップ表示されます。[Interface]ドロップダウンリストから、指定したポートが手順2で選択したポートであることを確認します。それ以外の場合は、ドロップダウン矢印をクリックして右ポートを選択します。

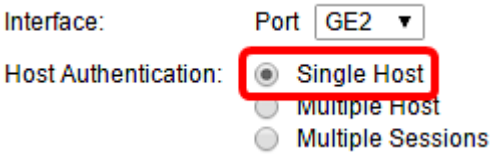


注：200または300シリーズを使用している場合は、[Edit Host and Session Authentication]ウィンドウが表示されます。

ステップ 5：[Host Authentication] フィールドで、目的の認証モードに対応するオプションボタンをクリックします。次のオプションがあります。

- Single Host：スイッチは、ポートへの単一の認可ホストアクセスのみを許可します。
- 複数のホスト(802.1X)：複数のホストが単一のポートにアクセスできます。これはデフォルト モードです。スイッチは最初のホストだけを認証する必要があり、その後、ポートに接続されている他のすべてのクライアントはネットワークにアクセスできます。認証に失敗すると、最初のホストと接続されているすべてのクライアントがネットワークへのアクセスを拒否されます。
- Multiple Sessions：複数のホストが1つのポートにアクセスできますが、各ホストは認証を受ける必要があります。

注：この例では、[Single host]が選択されています。

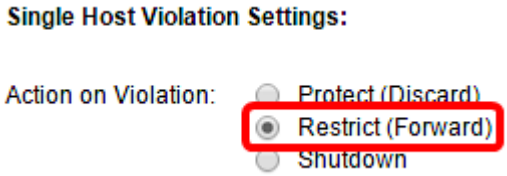


注：[Multiple Host]または[Multiple Sessions]を選択した場合は、ステップ9に進みます。

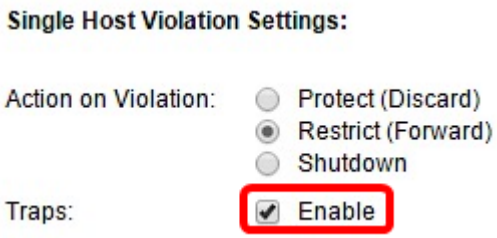
手順 6：[Host Violation Settings]領域で、目的の[Action on Violation]に対応するオプションボタンをクリックします。元のサプリカントのMACアドレスと一致しないMACアドレスを持つホストからパケットが到着すると、違反が発生します。これが発生すると、元のサプリカントと見なされていないホストから着信するパケットに対する処理が決定されます。次のオプションがあります。

- Protect(Discard)：パケットをドロップします。これはデフォルトのアクションです。
- Restrict(Forward)：アクセスを許可し、パケットを転送します。
- Shutdown：パケットをブロックし、ポートをシャットダウンします。ポートは、再アクティブ化されるか、スイッチがリブートされるまでダウンしたままになります。

注：この例では、[Restrict (Forward)]が選択されています。



ステップ7: (オプション) [Traps] フィールドの[Enable] をオンにして、トラップを有効にします。トラップは、システムイベントの報告に使用される簡易ネットワーク管理プロトコル(SNMP)メッセージを生成します。違反が発生すると、スイッチのSNMPマネージャにトラップが送信されます。



ステップ 8：[Trap Frequency] フィールドに、送信したトラップの間隔を秒単位で入力します。トラップの送信頻度を定義します。

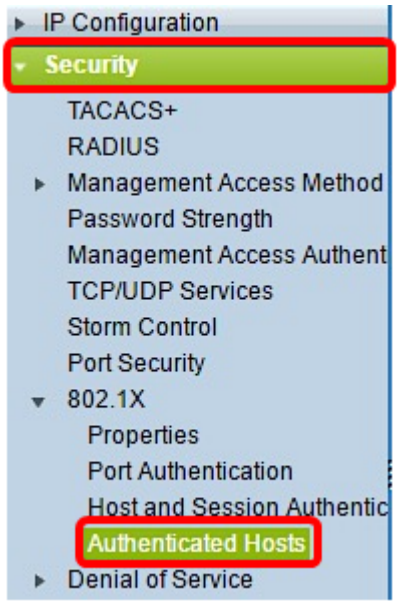
注：この例では、30秒が使用されています。

ステップ 9：[Apply] をクリックします。

これで、スイッチでホスト認証とセッション認証が設定されました。

認証されたホストの表示

ステップ 1：Webベースのユーティリティにログインし、[Security] > [802.1X] > [Authenticated Host] を選択します。



「認証されたホスト」テーブルには、認証されたホストに関する次の情報が表示されます。

- [User Name]：ポートで認証されたサプリカント名を指定します。
- Port：サプリカントが接続されるポート番号を指定します。
- Session Time：サプリカントがポートに接続された全時間を指定します。形式は DD:HH:MM:SS（日：時：分：秒）です。
- [Authentication Method]：認証に使用する方式を指定します。可能な値は次のとおりです。
- None：サプリカントが認証されなかったことを指定します。

- Radius：サプリカントがRADIUSサーバによって認証されたことを指定します。
- [MAC Address]：サプリカントのMACアドレスを指定します。
- VLAN ID：ホストが属するVLANを指定します。[VLAN ID]列は、220シリーズSmart Plusスイッチでのみ使用できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。