200/300シリーズマネージドスイッチでのアクセスプロファイルルールの設定

目的

アクセスプロファイルは、スイッチのセキュリティのもう1つのレイヤとして機能します。 アクセスプロファイルには、セキュリティを強化するために最大128のルールを含めることができます。各ルールには、アクションと基準が含まれています。アクセス方式が管理方式と一致しない場合、ユーザはブロックされ、スイッチにアクセスできません。

この記事では、200/300シリーズマネージドスイッチでプロファイルルールを設定する方法について説明します。

適用可能なデバイス

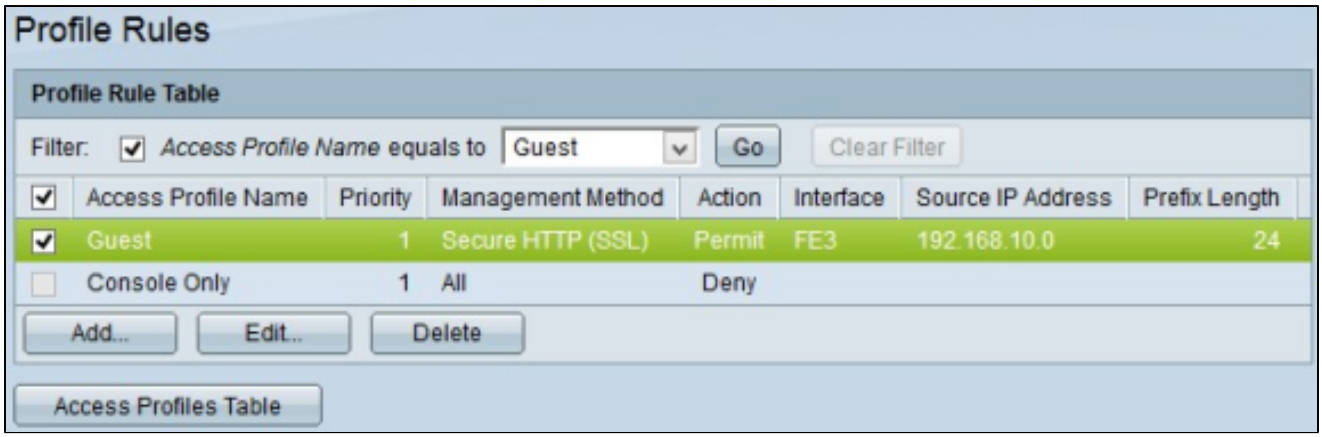
- SF/SG 200およびSF/SG 300シリーズマネージドスイッチ

[Software Version]

- v1.2.7.76

アクセスプロファイルの設定

ステップ 1：Web設定ユーティリティにログインし、Security > Mgmt Access Method > Profile Rulesの順に選択します。Profiles Rulesページが開きます。



ステップ 2：Filterチェックボックスをオンにして、Access Profileページで作成されたアクセスプロファイル名を表示します。

ステップ 3：Access Profile Name equals toドロップダウンリストから、目的のアクセスプロファイルを選択します。

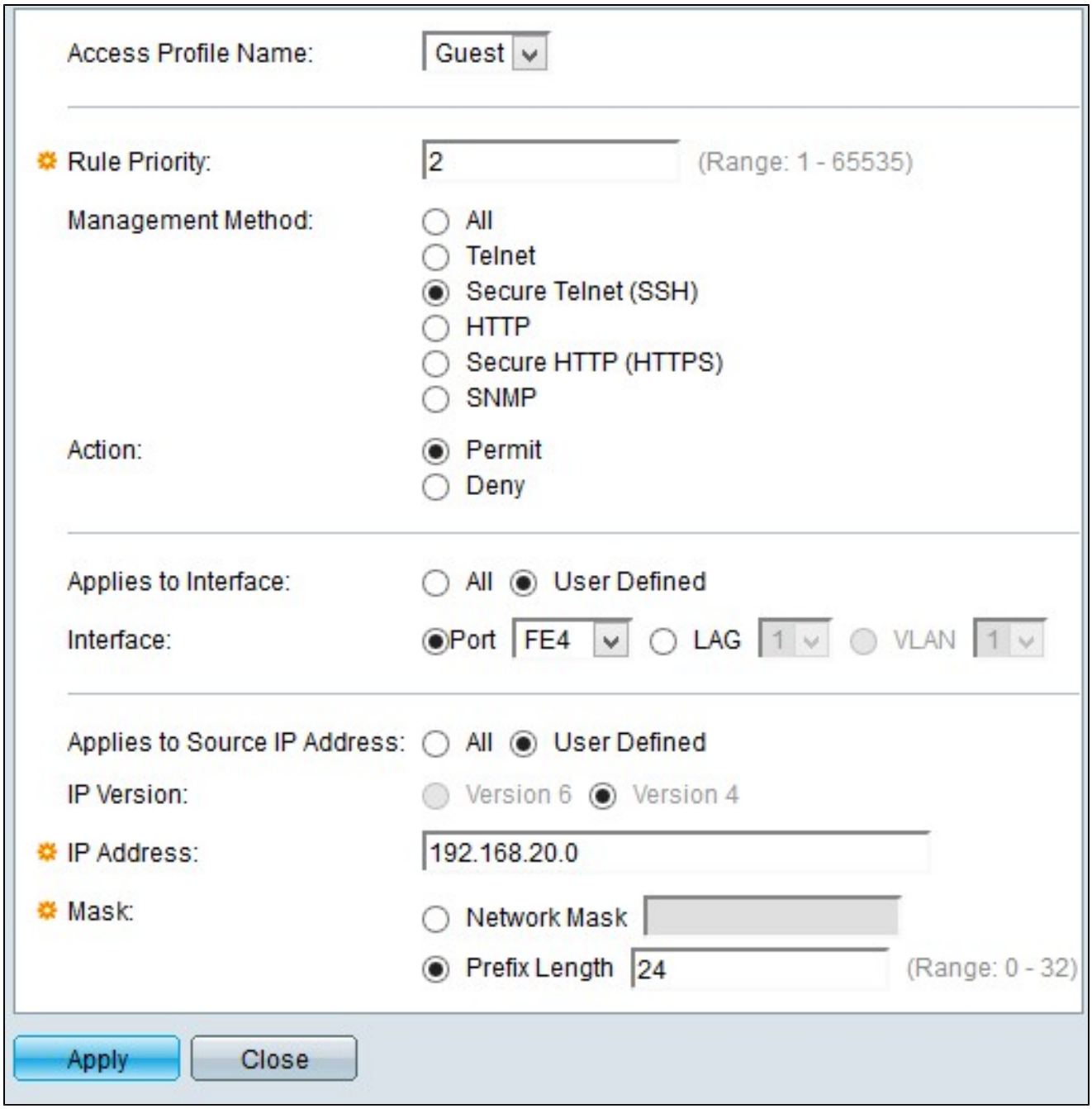
ステップ 4：Goをクリックして、目的のアクセスプロファイルを表示します。

ステップ5:（オプション）新しい検索を開始するには、Clear Filterをクリックします。

プロファイル規則の追加

ステップ 1：ルールを追加するアクセスプロファイルに対応するチェックボックスをオンにします。

ステップ 2：[Add] をクリックします。Add Profile Ruleウィンドウが表示されます。



ステップ3: (オプション) プロファイル規則を別のプロファイル名に追加するには、「アクセスプロファイル名」ドロップダウンリストから別のプロファイル名を選択します。

ステップ 4：Rule Priorityフィールドにルールの優先度を入力します。ルールの優先順位は、パケットとルールを一致させます。優先度の低いルールが最初にチェックされます。パケットがルールに一致すると、必要なアクションが実行されます。

ステップ 5：Management Methodフィールドで、目的の管理方法に対応するオプションボタンをクリックします。ユーザが使用するアクセス方式は、実行するアクションの管理方式と一致する必要があります。

- All：すべての管理方法がアクセスプロファイルに割り当てられます。

・ Telnet:Telnetの管理方法がルールに割り当てられています。Telnetミーティングアクセスプロファイル方式を持つユーザだけがデバイスにアクセスできます。

・ セキュアTelnet(SSH):SSH管理方式がプロファイルに割り当てられます。セキュアなTelnet会議アクセスプロファイルを持つユーザだけがデバイスにアクセスできます。

・ HTTP — HTTP管理方式がプロファイルに割り当てられます。HTTP会議アクセスプロファイル方式を使用するユーザのみがデバイスにアクセスできます。

・ セキュアHTTP(SSL):HTTPS管理方法がプロファイルに割り当てられます。HTTPS会議アクセスプロファイル方式を使用するユーザのみがデバイスにアクセスできます。

・ SNMP:SNMP管理方式がプロファイルに割り当てられます。SNMPミーティングアクセスプロファイル方式を使用するユーザのみがデバイスにアクセスできます。

手順 6：Actionオプションボタンから、ルールに添付するアクションを選択します。可能なアクション値は次のとおりです。

・ Permit：スイッチへのアクセスが許可されます。

・ Deny：スイッチへのアクセスが拒否されます。

手順 7：Applies to Interfaceフィールドで目的のインターフェイスタイプに対応するオプションボタンをクリックして、アクセスプロファイルのインターフェイスを定義します。

・ All：ポート、VLAN、LAGなどのすべてのインターフェイスが含まれます。

注:LAGは、より多くの帯域幅を提供するために複数の物理リンクを組み合わせる論理リンクです。

・ User Defined：ユーザの目的のインターフェイスにのみ適用されます。

- Port：アクセスプロファイルを定義するポートをPortドロップダウンリストから選択します。

- LAG:LAGドロップダウンリストから、アクセスプロファイルを定義するLAGドロップダウンリストからLAGを選択します。

- VLAN:VLANドロップダウンリストから、アクセスプロファイルを定義するVLANを選択

します。

ステップ 8：Source IP Addressオプションボタンをクリックして、インターフェイスの送信元IPアドレスを有効にします。次の2つの値が考えられます。

・ All：すべてのIPアドレスを含みます。

・ User Defined：ユーザの目的のIPアドレスにのみ適用されます。

– バージョン6:IPバージョン6アドレス用。

– バージョン4:IPバージョン4アドレス用。

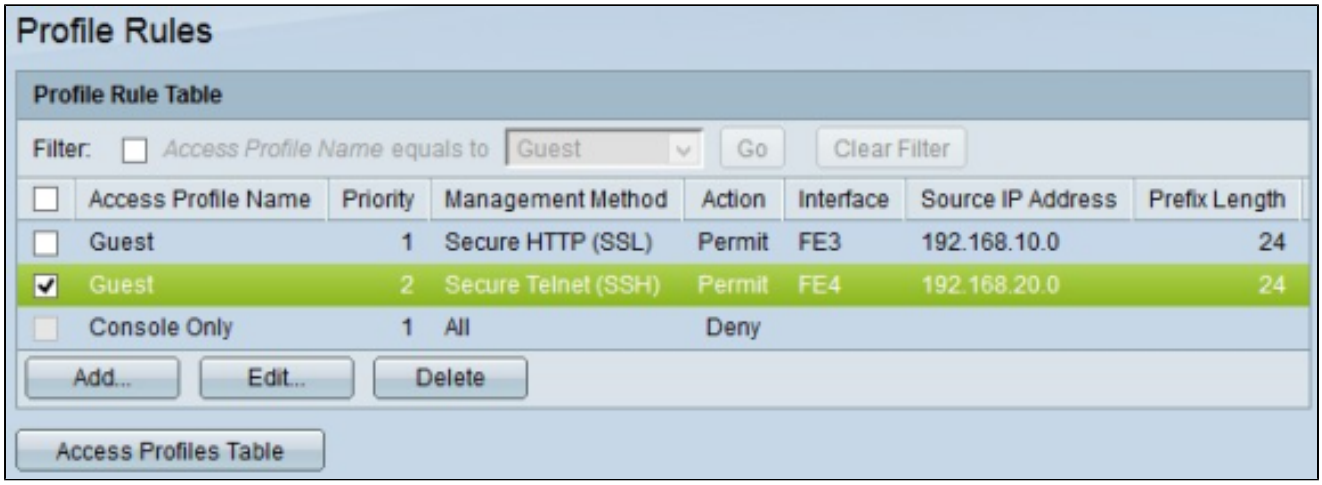
ステップ 9：ステップ7でUser Definedを選択した場合は、IP Addressフィールドにデバイスのアドレスを入力します。

ステップ 10：いずれかのオプションのMaskフィールドのオプションボタンをクリックして、ネットワークマスクを定義します。使用可能なオプションは次のとおりです。

・ ネットワークマスク：ドット付き10進表記でIPアドレスに対応するサブネットマスクを入力します。

・ Prefix Length:IPアドレスに対応するサブネットマスクのプレフィックス長を入力します。

ステップ 11[APPLY] をクリックします。



ステップ12:（オプション）現在のアクセスプロファイルを編集するには、編集するアクセ

スプロファイル名のチェックボックスをオンにして、Editをクリックします。

ステップ13. (オプション) アクセスプロファイルを削除するには、削除するアクセスプロファイルのチェックボックスをオンにして、Deleteをクリックします。

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。