300 シリーズによって管理されるスイッチのセキュリティ スイート設定

目標

サービス拒否（DoS）不正侵入からの Cisco 300 シリーズ管理されたスイッチ提供保護のセキュリティ スイート。 DoS攻撃は偽トラフィックとネットワークにあふれます、ネットワークサーバ リソースを正規のユーザに利用できなくか無理解にさせる。 通常、DoS攻撃には 2 つの型があります。 Brute Force DoS攻撃はサーバにあふれ、サーバおよびネットワーク帯域幅を消費します。 組織的不正侵入はシステムをクラッシュするために TCP SYN メッセージのようなプロトコル脆弱性を処理します。 この記事は 300 シリーズによって管理されるスイッチのセキュリティ スイートで利用可能 な設定を説明します。

注: DoS攻撃 保護が有効に なるときアクセス コントロール リスト（ACL）および高度 QoS ポリシーはポートで非アクティブです。

適当なデバイス

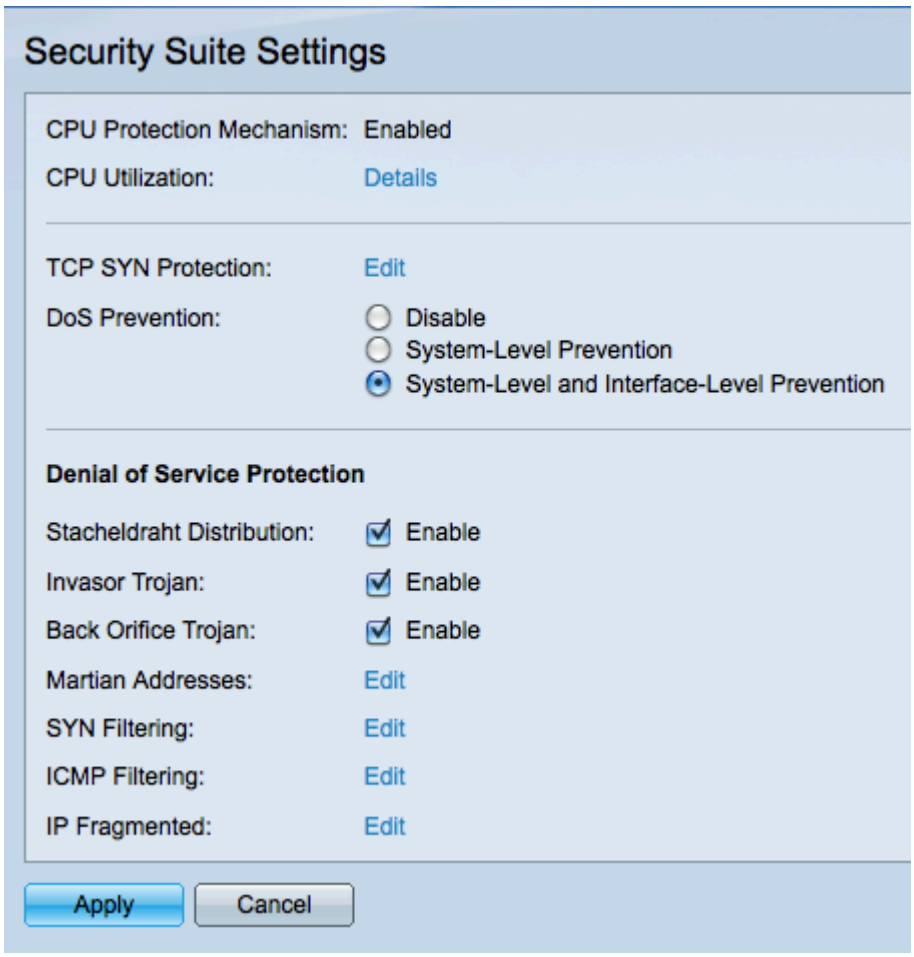
- SF/SG 300 シリーズによって管理されるスイッチ

[Software Version]

- 1.3.0.62

セキュリティ スイート設定設定

ステップ 1. Web コンフィギュレーションユーティリティへのログインは **> Denial of Service（DoS/DDoS）防止 > Security スイート設定**『Security』 を選択 し。 *Settings* ページ *セキュリティ スイートは*開きます:



注: CPU 保護メカニズムは 300 シリーズによって管理されるスイッチでデフォルトで有効に なり、無効に なることができません。 スイッチは多くのトラフィック総量が受信されてもいかにスイッチが管理およびプロトコル トラフィックを処理するようにするセキュア コア 技術（SCT）を使用します。

ステップ 2.（オプションの）は **CPU稼働率 フィールドで CPU稼働率を表示するために『Details』 をクリック します。** 詳細については *200/300 シリーズによって管理されるスイッチの*記事 *CPU稼働率*を参照して下さい。

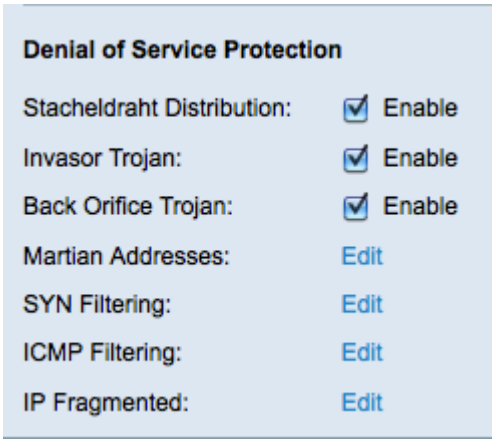
ステップ 3.（オプションの）は **TCP SYN 保護 フィールドで TCP SYN 保護設定を編集するために『Edit』 をクリック します。** 記事を*同期します（*詳細については *300 シリーズによって管理されるスイッチの SYN）フィルター構成*を参照して下さい。

ステップ 4 DoS 防止フィールドで、用いることを望む DoS 防止の方式に対応する Radio ボタンをクリックして下さい。 利用可能 な オプションは次のとおりです:

- disable — ディセーブル DoS 記憶保護機構。 ディセーブルが選択される場合、ステップ 13 にスキップして下さい。

- システム-レベル防止— Invasor トロイの木馬、Stacheldraht ディストリビューション、背部開口部トロイの木馬および火星人アドレスから保護する DoS 記憶保護機構を有効にします。

- システム-レベル防止および Interface-Level 保護— Denial of Service（DoS/DDoS）定義されるすべてのセキュリティ対策を保護 エリアで有効に します。



ステップ 5 16660 の出典 TCPポート番号の TCP パケットを廃棄するために Stacheldraht ディストリビューション フィールドの **Enable チェックボックスを**チェックして下さい。

ステップ 6 2140 の宛先TCP ポートが付いている TCP パケットおよび 1024 の出典 TCPポートを廃棄するために Invasor トロイ フィールドの **Enable チェックボックスを**チェックして下さい。

ステップ 7 31337 と等しい宛先 UDP ポートおよび 1024 の出典 UDP ポートが付いている UDP パケットを廃棄するために背部開口部トロイ フィールドの **Enable チェックボックスをチェックして下さい。**

注: 何百もの DoS攻撃の間、上記されるポートは悪意のあるアクティビティのために一般に不正利用されます。 ただし、それらはまた正当なトラフィックのために同様に使用されます。 上記のいずれかのポートを使用するデバイスがあれば、その情報はブロックされます。

ステップ 8.火星人アドレス・テーブルを編集するために火星 Addresses フィールドで『Edit』 をクリック して下さい。 火星人アドレス・テーブル破棄パケットはからの IP アドレスを選択します。 火星人アドレスのリストを編集するために、*300 シリーズによって管理されるスイッチの*記事 *サービス拒否（DoS）火星アドレス設定*を参照して下さい。

注: ステップは 9-12 システム レベルを必要とし、別の DoS 防止型を選択する場合 Interface-Level 防止はステップ 13 にステップ 4.でスキップします選択されます。

ステップ 9.管理者をある特定の TCP ポートをブロックすることを許可するために SYN フィルタリング フィールドで『Edit』 をクリック して下さい。 SYN フィルタリングを設定するために、*300 シリーズによって管理されるスイッチの*記事 *サービス拒否（DoS）SYN フィルター構成*を参照して下さい。

ステップ 10.受信される Syn パケットの数を制限するために SYN 比率 保護 フィールドで『Edit』 をクリック して下さい。 SYN 比率 保護を設定するために、*300 シリーズによって管理されるスイッチの*記事 *SYN 比率 保護*を参照して下さい。

ステップ 11.ある特定の出典からの ICMPパケットがブロックされるように ICMP フィルタリング フィールドで『Edit』 をクリック して下さい。 ICMP フィルタリングを設定するために、*300 シリーズによって管理されるスイッチの*記事 *インターネット制御メッセージ プロトコル（ICMP）フィルター構成*を参照して下さい。

ステップ 12： フラグメント化された IP パケットをブロックするために IP によってフラグメント化されるフィールドで『Edit』 をクリック して下さい。 フィルタリングする IP フラグメントを設定するために *300 シリーズによって管理されるスイッチの*記事 *サービス拒否*

*（DoS）IP フラグメント フィルター構成*を参照して下さい。

ステップ 13： 変更を保存するか、または変更を取り消すために『Cancel』 をクリック するために『Apply』 をクリック して下さい。