Cisco Intrusion Detection System の設定

- Cisco Intrusion Detection System について，1 ページ
- その他の情報，2 ページ
- IDS センサーの設定（GUI），2 ページ
- 回避クライアントの表示（GUI），3 ページ
- IDS センサーの設定（CLI），3 ページ
- 回避クライアントの表示（CLI），5 ページ

Cisco Intrusion Detection System について

Cisco Intrusion Detection System/Intrusion Prevention System（CIDS/IPS）は、特定のクライアントに関わる攻撃がレイヤ 3 ～ レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレスネットワークへのアクセスをブロックするよう、コントローラに指示します。 このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー
- IDS シグニチャ

ネットワークのさまざまなタイプの IP レベル攻撃を検出するように、IDS センサーを設定することができます。 センサーで攻撃が特定されたら、違反クライアントを回避（shun）するよう、コントローラに警告することができます。 新しく IDS センサーを追加したときは、コントローラをその IDS センサーに登録し、回避クライアントのリストをセンサーから取得できるようにします。

回避クライアント

IDS センサーは、疑わしいクライアントを検出すると、コントローラにこのクライアントを回避するよう警告します。 回避エントリは、同じモビリティ グループ内のすべてのコントローラに配

信されます。 回避すべきクライアントが現在、このモビリティ グループ内のコントローラに join している場合、アンカー コントローラはこのクライアントを動的除外リストに追加し、外部コントローラはクライアントを切り離します。 次回、このクライアントがコントローラに接続を試みた場合、アンカー コントローラはハンドオフを拒否し、外部コントローラにクライアントを除外することを通知します。

その他の情報

コントローラでは Cisco Prime Infrastructure を介して Cisco Wireless Intrusion Prevention System（wIPS）もサポートされています。 詳細については、「wIPS の設定」の項を参照してください。

IDS センサーの設定（GUI）

ステップ 1 [Security] > [Advanced] > [CIDs] > [Sensors] の順に選択して、[CIDS Sensors List] ページを開きます。

（注） 既存のセンサーを削除するには、そのセンサーの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 2 リストに新しい IDS センサーを追加するには、[New] をクリックします。 [CIDS Sensor Add] ページか表示されます。

ステップ 3 [Index] ドロップダウン リストから数字（1 ～ 5）を選択し、コントローラで IDS センサーが検索される順序を決定します。 たとえば、1 を選択した場合には、コントローラは最初にこの IDS センサーを検索します。
コントローラでは最大 5 つの IDS センサーをサポートします。

ステップ 4 [Server Address] テキスト ボックスに、IDS サーバの IP アドレスを入力します。

ステップ 5 [Port] テキスト ボックスに、コントローラが IDS センサーとの通信に使用する必要がある HTTPS ポートの番号を入力します。
センサーはデフォルトで 443 を使用して通信するので、このパラメータを 443 に設定することをお勧めします。 デフォルト値は 443 で、範囲は 1 ～ 65535 です。

ステップ 6 [Username]テキストボックスに、コントローラがIDSセンサーの認証に使用するユーザ名を入力します。

例：

（注） このユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 7 [Password] テキスト ボックスと [Confirm Password] テキスト ボックスに、コントローラが IDS センサーの認証に使用するパスワードを入力します。

ステップ 8 [Query Interval] テキスト ボックスに、コントローラが IDS サーバで IDS イベントをクエリーする間隔（秒単位）を入力します。
デフォルトは 60 秒で、範囲は 10 ～ 3600 秒です。

ステップ 9 [State] チェックボックスをオンにしてコントローラをこの IDS センサーに登録するか、このチェックボックスをオフにして登録を解除します。 デフォルト値はディセーブルです。

ステップ 10 [Fingerprint] テキスト ボックスに、40 桁の 16 進数文字のセキュリティ キーを入力します。 このキーは、センサーの有効性の確認、およびセキュリティ攻撃の防止に使用されます。

（注） キー内にコロンが 2 バイト間隔で表記されるようにしてください。 たとえば AA:BB:CC:DD のように入力します。

ステップ 11 [Apply] をクリックします。 [CIDS Sensors List] ページのセンサーのリストに新しい IDS センサーが表示されます。

ステップ 12 [Save Configuration] をクリックします。

回避クライアントの表示（GUI）

ステップ 1 [Security] > [Advanced] > [CIDS] > [Shunned Clients] の順に選択して、[CIDS Shun List] ページを開きます。このページには、各回避クライアントの IP アドレスと MAC アドレス、IDS センサーの要求に応じてコントローラがクライアントのデータ パケットをブロックする期間、およびクライアントを検出した IDS センサーの IP アドレスが表示されます。

ステップ 2 必要に応じて [Re-sync] をクリックし、リストを削除およびリセットします。

（注） コントローラは、対応するタイマーが期限切れになっても、回避エントリに何も処理を行いません。回避エントリ タイマーは、表示用としてのみ保持されます。回避エントリはコントローラが IPS サーバをポーリングするたびにクリーン アップされます。 CIDS IPS サーバに接続できない場合、回避エントリはコントローラでタイム アウトが生じても削除されません。 回避エントリは、CIDS IPS サーバが再び動作し、コントローラが CIDS IPS サーバをポーリングするときにのみクリーンアップされます。

IDS センサーの設定（CLI）

ステップ 1 次のコマンドを入力して、IDS センサーを追加します。

config wps cids-sensor add index ids_ip_address username password。 index パラメータは、コントローラで IDS センサーが検索される順序を決定します。 コントローラでは最大 5 つの IDS センサーをサポートします。 数字（1 ～ 5）を入力してこのセンサーの優先順位を決定します。 たとえば、1 を入力した場合には、コントローラは最初にこの IDS センサーを検索します。

（注） ユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 2 （任意）次のコマンドを入力して、コントローラが IDS センサーとの通信に使用する HTTPS ポートの番号を指定します。
config wps cids-sensor port index port

port-number パラメータには、1 ～ 65535 の値を入力することができます。 デフォルト値は 443 です。 この手順は任意であり、デフォルト値の443を使用することをお勧めします。デフォルトでは、センサーはこの値を使用して通信します。

ステップ 3 次のコマンドを入力して、コントローラが IDS センサーで IDS イベントをクエリーする間隔を指定します。
config wps cids-sensor interval index interval

interval パラメータには、10 ～ 3600 秒の値を入力することができます。 デフォルト値は 60 秒です。

ステップ 4 次のコマンドを入力して、センサーの有効性の確認に使用する 40 桁の 16 進数文字から成るセキュリティキーを入力します。
config wps cids-sensor fingerprint index sha1 fingerprint

センサーのコンソール上で show tls fingerprint と入力すると、フィンガープリントの値を取得できます。

（注） キー内にコロン（:）が 2 バイト間隔で表記されるようにしてください（たとえば、AA:BB:CC:DD）。

ステップ 5 次のコマンドを入力して、IDS センサーへのこのコントローラの登録を有効または無効にします。
config wps cids-sensor {**enable** | **disable**} *index*

ステップ 6 次のコマンドを入力して、DoS 攻撃からの保護を有効または無効にします。
デフォルト値はディセーブルです。

（注） 潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように IDS を誘導する場合があります。 それによって、コントローラはこの正規のクライアントの接続を誤って解除し、DoS 攻撃が開始されます。 自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。 ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。 792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

ステップ 7 次のコマンドを入力して、設定を保存します。
save config

ステップ 8 次のコマンドのいずれかを入力して、IDS センサーの設定を表示します。

- **show wps cids-sensor summary**
- **show wps cids-sensor detail** index

ステップ 9 2 つ目のコマンドは、1 つ目のコマンドよりも詳細な情報を提供します。

ステップ 10 次のコマンドを入力して、自動免疫設定の情報を表示します。
show wps summary

以下に類似した情報が表示されます。

```
Auto-Immune
  Auto-Immune..................................... Disabled

Client Exclusion Policy
```

```
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
Signature Policy
  Signature Processing........................... Enabled
```

ステップ 11 次のコマンドを入力して、IDS センサー設定に関連するデバッグ情報を取得します。
debug wps cids enable

（注） センサーの設定を削除または変更するには、まず config wps cids-sensor disable index コマンドを入力して設定を無効にする必要があります。 そのあと、センサーを削除するには、config wps cids-sensor delete index コマンドを入力します。

回避クライアントの表示（CLI）

ステップ 1 次のコマンドを入力して、回避すべきクライアントのリストを表示します。
show wps shun-list

ステップ 2 次のコマンドを入力して、コントローラを、この回避リストに対応するモビリティ グループ内の他のコントローラに同期させます。
config wps shun-list re-sync

（注） コントローラは、対応するタイマーが期限切れになっても、回避エントリに何も処理を行いません。 回避エントリ タイマーは、表示用としてのみ保持されます。 回避エントリはコントローラが IPS サーバをポーリングするたびにクリーン アップされます。 CIDS IPS サーバに接続できない場合、回避エントリはコントローラでタイム アウトが生じても削除されません。 回避エントリは、CIDS IPS サーバが再び動作し、コントローラが CIDS IPS サーバをポーリングするときにのみクリーンアップされます。