IP ソース ガードの設定

IP ソース ガードの概要

IP ソース ガード

IP ソースガード（IPSG）を使用して、ホストがネイバーの IP アドレスを使用する場合にトラフィック攻撃を防ぐことができ、また、信頼できないインターフェイスで DHCP スヌーピングが有効な場合に、IP ソースガードを有効にできます。

インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。IP および MAC のフィルタリングでは、送信元 IP 検索および送信元 MAC 検索の組み合わせが使用されます。バインディングテーブル内の送信元 IP アドレスを使用する IP トラフィックは許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング（スタティック IP 送信元バインディング）があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSG は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

スタティック ホスト用 IP ソース ガード

Note スタティックホストの IPSG は、アップリンクポートまたはトランクポートでは使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソースバインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブルエントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポート セキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。スタック化環境では、アクティブスイッチのフェールオーバーが発生すると、メンバポートに接続されたスタティックホストの IP ソースガードエントリは、そのまま残ります。**show device-tracking database** EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。

Note 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソースアドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティング システムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新

しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエージング アウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッドインターフェイスで **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを入力すると、次のエラーメッセージが表示されます。

  ```
  Static IP source binding can only be configured on switch port.
  ```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。

- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。

Note IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。

- IP ソース ガード スマート ロギングを設定すると、指定されたアドレスや DHCP によって学習されたアドレス以外の送信元アドレスを持つパケットは拒否され、そのパケットの内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。

- スイッチスタックでは、IP ソースガードがスタック メンバ インターフェイスに設定されていて、**no switch** *stack-member-number* **provision** グローバル コンフィギュレーション コマンドの入力によりそのスイッチの設定を削除した場合、インターフェイス スタティック バインディングはバインディングテーブルから削除されますが、実行コンフィギュレーションからは削除されません。**switch** *stack-member-number* **provision** コマンドを入力することによって、スイッチを再度プロビジョニングした場合、バインディングは復元されます。

実行コンフィギュレーションからバインディングを削除するには、**no switch provision** コマンドを入力する前に IP ソースガードを無効化する必要があります。インターフェイスがバインディングテーブルから削除される間にスイッチがリロードされると、設定も削除されます。

IP ソース ガードの設定方法

IP ソース ガードのイネーブル化

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **Example:** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip verify source** [**mac-check**] **Example:** `Device(config-if)# ip verify source`	送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。 （任意）**mac-check**：送信元 IP アドレスによる IP ソースガードおよび MAC アドレスフィルタリングを有効にします。
ステップ 5	**exit** **Example:** `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **Example:** `Device(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1`	スタティック IP ソース バインディングを追加します。 スタティック バインディングごとにこのコマンドを入力します。

	Command or Action	Purpose
ステップ 7	**end** **Example:** `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定

スタティックホスト用 IPSG を動作させるには、**ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。このコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルに有効にしていない、または IP device tracking maximum をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **Example:** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip device tracking** **Example:** `Device(config)# ip device tracking`	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルに有効にします。
ステップ 4	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	アクセスとしてポートを設定します。
ステップ 6	**switchport access vlan** *vlan-id* **Example:**	このポートに VLAN を設定します。

	Command or Action	Purpose
	`Device(config-if)# switchport access vlan 10`	
ステップ 7	**ip verify source**[**tracking**] [**mac-check**] **Example:** `Device(config-if)# ip verify source tracking mac-check`	送信元 IP アドレス フィルタリングによる IP ソース ガードを有効にします。 （任意）**tracking**：スタティックホスト用 IP ソースガードを有効にします。 （任意）**mac-check**：MACアドレスフィルタリングを有効にします。 **ip verify source tracking mac-check** コマンドは、MACアドレス フィルタリングのあるスタティック ホストに対して IP ソース ガードを有効にします。
ステップ 8	**ip device tracking maximum** *number* **Example:** `Device(config-if)# ip device tracking maximum 8`	そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ～ 10 です。最大値は 10 です。 **Note** **ip device tracking maximum** *limit-number* インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 9	**end** **Example:** `Device(config-if)# end`	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP ソース ガードのモニタリング

表 *1*：特権 *EXEC* 表示コマンド

コマンド	目的
show ip verify source [**interface** *interface-id*]	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。
show ip device tracking { **all** | **interface** *interface-id* | **ip** *ip-address* | **mac** *mac-address*}	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

表 *2:* インターフェイス コンフィギュレーション コマンド

コマンド	目的
ip verify source tracking	データ ソースを確認します。

IP ソース ガードの機能の履歴

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 Everest 16.5.1a	IP ソース ガード	ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

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。