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

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。

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 検索が組み合わせが使用されます。送信元 IP アドレスを使用する IP トラフィックでは、バインディングテーブルが許可され、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

（注） アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード（IPSG）を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、マスター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** 特権 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。

（注） 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。

（注） 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 メンバー インターフェイスに設定されていて、**noswitch** *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 ガードをディセーブルに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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。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	**configureterminal** 例： `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* 例： `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	**exit** 例： `Device(config-if)# exit`	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 5	**ip source binding** *mac-address***vlan** *vlan-id ip-address***interface** *interface-id* 例： `Device(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4`	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。

	コマンドまたはアクション	目的
	interface gigabitethernet1/0/1	
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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 trackingmaximum** *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イネーブルにしていない、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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `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** 例： `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* 例： `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** 例： `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* 例： `Device(config-if)# switchport access vlan 10`	このポートに VLAN を設定します。
ステップ 7	**ip device tracking maximum** *number* 例： `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。 （注） **ip device trackingmaximum** *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 8	**end** 例： `Device(config)# end`	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** *imac-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。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

その他の参考資料

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IP ソース ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよび Cisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3* : *IP* ソース ガードの機能情報

機能名	リリース	機能情報
IP ソース ガード	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ