IP ソース ガードの設定

IP ソース ガード（IPSG）は、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 トラフィックを制限するセキュリティ機能で、DHCP スヌーピング バインディング データベースと手動で設定された 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することで実現されます。

この章は、次の内容で構成されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ 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 には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

IP ソース ガードの概要

IPSG

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 ip device tracking all** 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。

- EtherChannels では、IP ソース ガードはサポートされません。
- 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、**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

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **ip verify source**［**mac-check** ］
4. **exit**
5. **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**interface** *interface-id* 例： `Switch(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 3	**ip verify source**［**mac-check** ］ 例： `Switch(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 ガードをイネーブルにします。 （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 フィルタリングをイネーブルにします。
ステップ 4	**exit** 例： `Switch(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*	スタティック IP ソース バインディングを追加します。

	コマンドまたはアクション	目的
	例： `Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1`	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。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

VLAN 10 および 11 上の送信元 IP および MAC アドレスのフィルタリングを使用した IP ソース ガードのイネーブル化

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# ip verify source
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet
 1/0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet
 1/0/1
Switch(config)# end
```

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。

手順の概要

1. **configure terminal**
2. **ip device tracking**
3. **interface** *interface-id*
4. **switchport mode access**
5. **switchport access vlan** *vlan-id*
6. **ip verify source**[**tracking**] [**mac-check**]
7. **ip device tracking maximum** *number*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**ip device tracking** 例： `Switch(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イネーブルにします。
ステップ 3	**interface** *interface-id* 例： `Switch(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 4	**switchport mode access** 例： `Switch(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 5	**switchport access vlan** *vlan-id* 例： `Switch(config-if)# switchport access vlan 10`	このポートに VLAN を設定します。

	コマンドまたはアクション	目的
ステップ 6	**ip verify source**[**tracking**] [**mac-check**] 例： `Switch(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 ガードをイネーブルにします。 （任意）**tracking**：スタティック ホスト用 IP ソース ガードをイネーブルにします。 （任意）**mac-check**：MAC アドレス フィルタリングをイネーブルにします。 **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 ガードをイネーブルにします。
ステップ 7	**ip device tracking maximum** *number* 例： `Switch(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 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 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

8 つの例

次に、インターフェイス上でスタティック ホストを使って IPSG を停止する例を示します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

次に、ポート上でスタティック ホストを使って IPSG をイネーブルにする例を示します。

```
Switch(config)# ip device tracking
Switch(config-if)# ip device tracking maximum 10
Switch(config-if)# ip verify source tracking
```

次に、レイヤ 2 アクセス ポートに対してスタティック ホストの IPSG と IP フィルタをイネーブルにしてから、インターフェイス Gi1/0/3 上の有効な IP バインディングを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# ip device tracking maximum 5
```

```
Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       40.1.1.24                          10
Gi1/0/3      ip trk       active       40.1.1.20                          10
Gi1/0/3      ip trk       active       40.1.1.21                          10
```

次に、レイヤ2アクセスポートに対してスタティックホストのIPSGとIP-MACフィルタをイネーブルにしてから、インターフェイスGi1/0/3上の有効なIP-MACバインディングを確認し、さらにこのインターフェイス上のバインディングの数が最大値に達しているかどうかを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5

Switch(config-if)# ip verify source tracking
Switch(config-if)# end

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi1/0/3      ip trk       active       deny-all                           1
```

この例は、すべてのインターフェイスに対するIPまたはMACバインディング エントリをすべて表示します。CLIはアクティブエントリと非アクティブエントリの両方を表示します。インターフェイスでホストが学習されると、この新しいエントリは、アクティブとマークされます。 このホストをこのインターフェイスから切断し、別のインターフェイスに接続すると、ホストを検出すると同時に、新しいIPまたはMACバインディング エントリがアクティブとして表示されます。 以前のインターフェイスでは、このホストに対する古いエントリが非アクティブとマークされます。

```
Switch# show ip device tracking all
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------------------------------

  IP Address     MAC Address   Vlan  Interface           Probe-Timeout      STATE
-----------------------------------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.9       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.10      0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.1       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.1       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.2       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.2       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.3       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.3       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.4       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.4       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.5       0001.0600.0000  9   GigabitEthernet1/0/2                   ACTIVE
200.1.1.5       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.6       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
200.1.1.7       0001.0600.0000  8   GigabitEthernet1/0/1                   INACTIVE
```

この例は、すべてのインターフェイスに対するアクティブな IP または MAC バインディング エントリをすべて表示します。

```
Switch# show ip device tracking all active
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients = Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------------------------------

  IP Address     MAC Address   Vlan  Interface           Probe-Timeout      STATE
-----------------------------------------------------------------------------------------------
200.1.1.1       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.2       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.3       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.4       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
200.1.1.5       0001.0600.0000  9    GigabitEthernet1/0/1                  ACTIVE
```

この例は、すべてのインターフェイスに対する非アクティブな IP または MAC バインディング エントリをすべて表示します。 このホストは、初めに GigabitEthernet 1/0/1 上で学習され、その後で GigabitEthernet 0/2 に移動しました。 GigabitEthernet1/0/1 上で学習された IP または MAC バインディング エントリは、非アクティブとなっています。

```
Switch# show ip device tracking all inactive
IP Device Tracking for wireless clients = Enabled
Global IP Device Tracking for wired clients= Enabled
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------------------------------------

  IP Address     MAC Address   Vlan  Interface           Probe-Timeout      STATE
-----------------------------------------------------------------------------------------------
200.1.1.8       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.9       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.10      0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.1       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.2       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.3       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.4       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.5       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.6       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
200.1.1.7       0001.0600.0000  8    GigabitEthernet1/0/1                  INACTIVE
```

この例は、すべてのインターフェイスに対するすべての IP デバイス トラッキング ホスト エントリの総数を表示します。

```
Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5
-------------------------------------------------------------------
  Interface           Maximum Limit           Number of Entries
-------------------------------------------------------------------
Gi1/0/3                  5
```

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 がソース トラッキングを確認	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。

Additional References

MIBs

MIB	MIBs Link
本リリースでサポートするすべての MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support