IP ソース ガードの設定

この章では、Cisco NX-OS デバイスで IP ソース ガードを設定する手順について説明します。

この章は、次の項で構成されています。

IP ソース ガードについて

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP および MAC のアドレス バインディングのフィルタリングは、スプーフィング攻撃（有効なホストの IP アドレスを使用して不正なネットワーク アクセス権を取得する攻撃）の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

DHCP スヌーピングで信頼状態になっていないレイヤ 2 インターフェイスの IP ソース ガードをイネーブルにできます。IP ソース ガードは、アクセス モードとトランク モードで動作するように設定されているインターフェイスをサポートしています。IP ソース ガードを最初にイ

ネーブルにすると、次のトラフィックを除いて、そのインターフェイス上のインバウンド IP トラフィックがすべてブロックされます。

- DHCP パケット。DHCP パケットは、DHCP スヌーピングによって検査が実行され、その結果に応じて転送またはドロップされます。
- Cisco NX-OS デバイスに設定したスタティック IP ソース エントリからの IP トラフィック。

デバイスが IP トラフィックを許可するのは、DHCP スヌーピングによって IP パケットの IP アドレスと MAC アドレスのバインディング テーブル エントリが追加された場合、またはユーザがスタティック IP ソース エントリを設定した場合です。

パケットの IP アドレスと MAC アドレスがバインディング テーブル エントリにも、スタティック IP ソース エントリにもない場合、その IP パケットはドロップされます。たとえば、**show ip dhcp snooping binding** コマンドによって表示されたバインディング テーブル エントリが次のとおりであるとします。

```
MacAddress          IpAddress    LeaseSec   Type           VLAN    Interface
------------------  ----------   ---------  -------------  ----    ---------
00:02:B3:3F:3B:99   10.5.5.2     6943       dhcp-snooping  10      Ethernet2/3
```

IP アドレスが 10.5.5.2 の IP パケットをデバイスが受信した場合、IP ソース ガードによってこのパケットが転送されるのは、このパケットの MAC アドレスが 00:02:B3:3F:3B:99 のときだけです。

IP ソース ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- IP ソース ガードを設定するには、その前に DHCP 機能および DHCP スヌーピングをイネーブルにする必要があります。DHCP の設定を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、IP ソース ガード用の ACL TCAM のリージョン サイズを設定する必要があります。ACL TCAM リージョン サイズの設定を参照してください。

Note デフォルトでは、ipsg のリージョン サイズはゼロです。SMAC-IP バインディングの保存と適用をするには、このリージョンに十分なエントリを割り当てる必要があります。

IP ソース ガイドの注意事項と制約事項

IP ソース ガードに関する注意事項と制約事項は次のとおりです。

- IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリまたはスタティック IP ソース エントリに送信元が含まれているトラフィックだけに制限します。インターフェイス上の IP ソース ガードを初めてイネーブルにする際には、そのインターフェイス上のホストが DHCP サーバから新しい IP アドレスを受信するまで、IP トラフィックが中断されることがあります。
- IP ソース ガードの機能は、DHCP スヌーピング（IP-MAC アドレス バインディング テーブルの構築および維持に関して）、またはスタティック IP ソース エントリの手動での維持に依存しています。
- IP ソース ガードは、Fabric Extender（FEX）および汎用拡張モジュール（GEM）ポートではサポートされていません。
- 次の注意事項と制約事項は、Cisco Nexus 9200 シリーズ スイッチに適用されます。
  - 着信インターフェイスで IPSG がイネーブルであると IPv6 の隣接関係は形成されません。
  - IPSG は HSRP スタンバイで ARP パケットを廃棄します。
  - DHCP スヌーピングおよび IPSG がイネーブルにされている場合、ホストのバインディング エントリが存在すると、ARP がなくてもトラフィックはホストに転送されます。
- Cisco NX-OS リリース 9.3(5) 以降、IP Source Guard は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。

IP ソース ガードのデフォルト設定

次の表に、IP ソース ガードのパラメータのデフォルト設定を示します。

***Table 1: IP* ソース ガードのパラメータのデフォルト値**

パラメータ	デフォルト
IP ソース ガード	各インターフェイスでディセーブル
IP ソース エントリ	なし。デフォルトではスタティック IP ソース エントリはありません。デフォルトの IP ソース エントリもありません。

IP ソース ガードの設定

レイヤ2インターフェイスに対するIPソース ガードのイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対して IP ソース ガードをイネーブルまたはディセーブルに設定できます。デフォルトでは、すべてのインターフェイスに対して IP ソース ガードはディセーブル。

Before you begin

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

IPSG（ipsg）の ACL TCAM リージョン サイズが設定されていることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		指定したインターフェイスのインターフェイス 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	[**no**] **ip verify source dhcp-snooping-vlan** **Example:** `switch(config-if)# ip verify source dhcp-snooping vlan`	インターフェイスの IP ソース ガードをイネーブルにします。このコマンドの **no** 形式を使用すると、そのインターフェイスの IP ソース ガードがディセーブルになります。
ステップ 4	(Optional) **show running-config dhcp** **Example:** `switch(config-if)# show running-config dhcp`	IP ソース ガードの設定も含めて、DHCP スヌーピングの実行コンフィギュレーションを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スタティック IP ソース エントリの追加または削除

デバイス上のスタティック IP ソース エントリの追加または削除を実行できます。デフォルトでは、固定 IP ソース エントリは作成されません。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **ip source binding** *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-type slot*/*port* **Example:** `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	現在のインターフェイスのスタティック IP ソース エントリを作成します。このコマンドの **no** 形式を使用すると、スタティック IP ソース エントリが削除されます。
ステップ 3	(Optional) **show ip dhcp snooping binding** [**interface** *interface-type slot*/*port*] **Example:** `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレス バインディングを表示します。スタティック エントリは、Type カラムの表示で示されます。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トランク ポート用 IP ソース ガードの設定

あるポートに IP ソース ガードが設定されている場合、それを TCAM 内で許可する DHCP スヌーピング エントリがない限り、そのポートに着信するトラフィックはドロップされます。ただし、IP ソース ガードがトランク ポートに設定されていて特定の VLAN で着信するトラフィックではこのチェックを行いたくない場合（それらで DHCP スヌーピングがイネーブルにされていない場合であっても）、除外したい VLAN のリストを指定できます。

始める前に

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

手順

	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`
	`switch(config)#`
		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	[**no**] **ip dhcp snooping ipsg-excluded vlan** *vlan-list* 例： `switch(config)# ip dhcp snooping ipsg-excluded vlan 1001-1256,3097`	トランク ポートの IP ソース ガードで DHCP スヌーピングのチェックから除外したい VLAN のリストを指定します。
ステップ 3	（任意） **show ip ver source** [**ethernet** *slot/port* | **port-channel** *channel-number*] 例： `switch(config)# show ip ver source`	どの VLAN が除外されるかを表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ソース ガード バインディングの表示

show ip ver source [**ethernet** *slot/port* | **port-channel** *channel-number*] を使用します コマンドを使用して、IP-MAC アドレスのバインディングを表示します。

IP ソース ガードの統計情報のクリア

IP ソース ガードの統計情報のクリアを行うには、次の表に示すコマンドを使用します。

コマンド	目的
clear access-list ipsg stats [**instance** *number* | **module** *number*]	IP ソース ガードの統計情報をクリアします。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成し、インターフェイスの IP ソース ガードをイネーブルにする例を示します。

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
  show ip ver source

  IP source guard excluded vlans:
  -------------------------------------------------------
  None

  -----------------------------------
  IP source guard is enabled on the following interfaces:
  -------------------------------------------------------
        ethernet2/3
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	IP ACL の設定
『DHCP and DHCP snooping』	DHCP の設定

関連資料