CHAPTER 14

IP ソース ガードの設定

この章では、Cisco Nexus 1000V 上で 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、次の内容で構成されています。

IP ソース ガードの概要

IP ソース ガードとは、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、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング テーブル内のダイナミックまたはスタティック IP ソース エントリの IP-MAC アドレス バインディングと一致する場合にのみ、IP トラフィックを許可します。

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 Nexus 1000V 内で設定済みのスタティック 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      vEthernet3
```

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 ガードを設定するためには、DHCP スヌーピングについての知識が必要です。
- DHCP スヌーピングがイネーブルになっている必要があります（「DHCP スヌーピングの設定」（P.12-4）を参照）。

注意事項および制約事項

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。DHCP スヌーピングの詳細については、第 12 章「DHCP スヌーピングの設定」を参照してください。
- IP ソース ガードをシームレスにするために、仮想サービス ドメイン（VSD）サービス VM ポートは、デフォルトで信頼できるポートとなっています。これらのポートを「信頼できない」と設定しても、その設定は無視されます。

デフォルト設定

表 14-1 に、IP ソース ガードのデフォルトを示します。

表 14-1　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
IPSG	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

ここでは、次の内容について説明します。

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

ここでは、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する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- 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。
- DHCP スヌーピングがイネーブルになっていることを確認してください。詳細については、「DHCP 機能のイネーブル化またはディセーブル化」（P.12-5）を参照してください。

手順の概要

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. **[no] ip verify source dhcp-snooping-vlan**
4. **show running-config dhcp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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 vethernet** *interface-number*
	
	例：
	`switch(config)# interface vethernet 3`
	`switch(config-if)#`
		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。*interface-number* は、DHCP スヌーピングにおいて信頼できるものとして扱うかどうかを設定する vEthernet インターフェイスです。

	port-profile *profilename*
	
	例：
	`switch(config)# port-profile vm-data`
	`switch(config-port-prof)#`
		指定したポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。*profilename* は最大 80 文字の一意の名前です。

	コマンド	目的
ステップ 3	[no] **ip verify source dhcp-snooping-vlan** **例：** `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。**no** オプションを使用すると、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	**show running-config dhcp** **例：** `switch(config-if)# show running-config dhcp`	（任意）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。IP ソース ガードの設定も表示されます。
ステップ 5	**copy running-config startup-config** **例：** `switch(config-if)# copy running-config startup-config`	（任意）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

ここでは、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の手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- デフォルトでは、デバイスにはスタティック IP ソース エントリは設定されていません。

手順の概要

1. **config t**
2. [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface vethernet** *interface-number*
3. **show ip dhcp snooping binding [interface vethernet** *interface-number*]
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： switch# config t 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 vethernet** *interface-number* 例： switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 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。スタティック IP ソース エントリを削除する場合は、**no** オプションを使用します。
ステップ 3	**show ip dhcp snooping binding** [**interface vethernet** *interface-number*] 例： switch(config)# show ip dhcp snooping binding interface ethernet 3	（任意）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 IP ソース エントリも表示されます。スタティック エントリは、Type カラムに「static」と表示されます。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）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 ガードの設定の確認

IP ソース ガードの設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。
show ip verify source	IP-MAC アドレス バインディングを表示します。

コマンド出力の詳しい説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

IP ソース ガード バインディングの表示

IP-MAC アドレス バインディングを表示するには、**show ip verify source** コマンドを使用します。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成してから、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 vethernet 3
interface ethernet 2/3
  no shutdown
  ip verify source dhcp-snooping-vlan
```

その他の関連資料

IP ソース ガードの実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.14-6）
- 「標準」（P.14-6）

関連資料

関連項目	参照先
「DHCP スヌーピングの概要」（P.12-1）	『*Cisco Nexus 1000V セキュリティ コンフィギュレーション ガイド リリース 4.2(1)SV1(5.1)*』、*第 12 章「DHCP スヌーピングの設定」*
IP ソース ガード コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』
DHCP スヌーピングのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ソース ガードの機能の履歴

表 14-2 は、この機能のリリースの履歴です。

表 14-2　IP ソース ガードの機能の履歴

機能名	リリース	機能情報
IPSG	4.0(4)SV1(2)	この機能が導入されました。