CHAPTER 19

DHCP、DAI、および IPSG

この章では、次のセキュリティ機能に関する問題を識別して解決する方法について説明します。

- Dynamic Host Configuration Protocol（DHCP）スヌーピング
- Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）
- IP Source Guard（IPSG; IP ソース ガード）

この章は、次の内容で構成されています。

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような役割を果たします。具体的には、次の処理を実行します。

- 信頼できない発信元からの DHCP メッセージを検証するとともに、DHCP サーバからの無効な応答メッセージを除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

DHCP スヌーピングの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

ダイナミック ARP インスペクションに関する情報

DAI は、ARP の要求と応答を検証するための機能です。具体的には、次のような処理を実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- ARP キャッシュの更新やパケットの転送を行う前に、そのパケットに対応する有効な IP-to-MAC バインディングが存在することを確認します。
- 無効な ARP パケットはドロップします。

DAI によって ARP パケットの有効性を判断するときの基準となる有効な IP-to-MAC バインディングは、Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング データベースに保存されています。このデータベースは、VLAN とデバイスに対して DHCP スヌーピングがイネーブルになっている場合に、DHCP スヌーピング機能によって構築されます。このデータベースには、管理者が作成したスタティック エントリが格納されていることもあります。

DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

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。

IP ソース ガードの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

トラブルシューティングの注意事項と制約事項

DHCP スヌーピング、ダイナミック ARP インスペクション、または IP ソース ガードをトラブルシューティングするときは、次の注意事項と制約事項が適用されます。

- 最大 2000 の DHCP エントリを DVS 内のシステム全体でスヌーピングまたは学習できます。これは、動的に学習されたエントリと、静的に設定されたエントリの両方を組み合わせた合計です。
- DHCP サーバに接続している VSD SVM ポートまたは vEthernet ポートなどの信頼できるインターフェイスについては、インターフェイスのレート制限値を高めに設定する必要があります。

これらの機能の設定に使用する詳細な注意事項および制約事項については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

DHCP スヌーピングの問題

次に、DHCP スヌーピングに関する問題の現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
スヌーピングが設定された状態では、DHCP クライアントはサーバから IP アドレスを取得できません。	IP アドレスがバインディング データベースに追加されていない。 DHCP サーバとクライアント間の接続の障害。	1. DHCP サーバと、クライアントに接続されているホスト間の接続を確認します。 **vmkping** 2. DHCP サーバとホスト間の接続が切断された場合は、次の手順を実行します。 – たとえば、VLAN が許可されているかなど、アップストリーム スイッチで設定を確認します。 – サーバ自体がアップし、稼動していることを確認します。
	VM として DVS に接続している DHCP サーバのインターフェイスが信頼できない。	1. VSM で、インターフェイスが信頼できることを確認します。 **show ip dhcp snooping** 2. VSM で、サーバに接続している vEthernet インターフェイスが信頼できることを確認します。 **module vem** *mod#* **execute vemcmd show dhcps interfaces**
	VM からの DHCP 要求がサーバに到達せず、肯定応答を得られない。	DHCP サーバで、ログインしてパケット キャプチャ ユーティリティを使用し、パケットの要求および確認応答を確認します。
	DHCP 要求と肯定応答が Cisco Nexus 1000V に到達していない。	• クライアント vEthernet インターフェイスから、パケットを SPAN で解析して、パケットがクライアントに到達していることを確認します。 • クライアントに接続されているホストで、VEM パケット キャプチャをイネーブルにし、パケットの着信要求および確認応答を確認します。
	Cisco Nexus 1000V が、パケットをドロップしている。	VSM で、DHCP 統計情報を確認します。 **show ip dhcp snooping statistics** **module vem** *mod#* **execute vemcmd show dhcps stats**

ドロップされた ARP 応答のトラブルシューティング

次に、ドロップされた ARP 応答の原因、および解決方法を示します。

考えられる原因	解決策
ARP インスペクションが VSM に設定されていない。	VSM で、ARP インスペクションが予期したとおりに設定されていることを確認します。 **show ip arp inspection** DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
DHCP スヌーピングが VSM でグローバルにイネーブルにならず、VLAN でもイネーブルにならない。	VSM で、DHCP スヌーピングの設定を確認します。 **show ip dhcp snooping** DHCP をイネーブルにして、DAI を設定する方法の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
DHCP スヌーピングが VEM でイネーブルにならず、VLAN でもイネーブルにならない。	1. VSM から、VEM の DHCP スヌーピングの設定を確認します。 **module vem** *mod#* **execute vemcmd show dhcps vlan** 2. 次のいずれかを実行します。 – VSM の DHCP 設定のエラーを修正します。詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。 – VSM の設定に誤りが見つからないが、VEM でエラーになる場合は、VSM と VEM の両方からエラー ログをキャプチャして分析し、エラーの理由を識別します。
スヌーピングがディセーブルである場合、バインディング エントリがバインディング テーブルに静的に設定されない。	1. VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** 2. スタティック バインディング テーブルのエラーを修正します。 テーブルからのエントリのクリア、DHCP のイネーブル化、および DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
ARP 応答を送信している VM に対応するバインディングが、バインディング テーブルに存在しない。	1. VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** 2. スタティック バインディング テーブルのエラーを修正します。 テーブルからのエントリのクリア、DHCP のイネーブル化、および DAI の設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。 3. どの設定にも誤りがない場合は、DAI または IPSG の前に DHCP スヌーピングをオンにしていることを確認します。これによって、Cisco Nexus 1000V はスヌーピング データベースにバインディングを追加するのに十分な時間を取ることができます。 詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。

IP ソース ガードの問題

次に、IP ソース ガードの問題について現象、考えられる原因、および解決方法を示します。

症状	考えられる原因	解決策
トラフィックの中断	ARP インスペクションが VSM に設定されていない。	VSM で、IP ソース ガードが予期したとおりに設定されていることを確認します。 **show port-profile name** *profile_name* **show running interface** *if_ID* **show ip verify source** IP ソース ガードの設定の詳細については、『*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
	vEthernet インターフェイスに対応する IP アドレスがスヌーピング バインディング テーブルにない。	1. VSM で、バインディング テーブルを表示します。 **show ip dhcp snooping binding** 2. 欠落しているスタティック エントリを設定するか、VM でリースを更新します。 3. VSM で、バインディング テーブルを再表示して、エントリが適切に追加されていることを確認します。 **show ip dhcp snooping binding**

ログの収集と評価

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、VSM からこの項のコマンドを使用します。

- 「VSM ロギング」（P.19-5）
- 「ホスト ロギング」（P.19-6）

VSM ロギング

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、VSM からこの項のコマンドを使用します。

VSM コマンド	説明
debug dhcp all	dhcp 設定フラグに対するすべてのデバッグをイネーブルにします。
debug dhcp errors	エラーのデバッグをイネーブルにします。
debug dhcp mts-errors	mts エラーのデバッグをイネーブルにします。
debug dhcp mts-events	mts イベントのデバッグをイネーブルにします。
debug dhcp pkt-events	pkt イベントのデバッグをイネーブルにします。

VSM コマンド	説明
debug dhcp pss-errors	pss エラーのデバッグをイネーブルにします。
debug dhcp pss-events	pss イベントのデバッグをイネーブルにします。

ホスト ロギング

DHCP、DAI、および IP ソース ガードに関するログを収集し、表示するには、ESX ホストからこの項のコマンドを使用します。

ESX ホスト コマンド	説明
echo "logfile enable" > /tmp/dpafifo	DPA デバッグ ロギングをイネーブルにします。 ログは、/var/log/vemdpa.log ファイルに出力されます。
echo "debug sfdhcpsagent all" > /tmp/dpafifo	DPA DHCP エージェント デバッグ ロギングをイネーブルにします。 ログは、/var/log/vemdpa.log ファイルに出力されます。
vemlog debug sfdhcps all	データパス デバッグ ロギングをイネーブルにして、クライアントとサーバ間で送信されたデータパケットに関するログをキャプチャします。
vemlog debug sfdhcps_config all	データパス デバッグ ロギングをイネーブルにして、VSM からの設定に関するログをキャプチャします。
vemlog debug sfdhcps_binding_table all	データパス デバッグ ロギングをイネーブルにして、バインディング データベースの変更に対応するログをキャプチャします。

DHCP、DAI、および IPSG のトラブルシューティング コマンド

DHCP スヌーピング、DAI、および IP ソース ガードに関する問題をトラブルシューティングするには、この項のコマンドを使用します。

コマンド	説明
show running-config dhcp	DHCP スヌーピング、DAI、および IP ソース ガードの設定を表示します。 例 19-1（P.19-7）を参照してください。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。 例 19-2（P.19-7）を参照してください。

コマンド	説明
show ip dhcp snooping binding	DHCP スヌーピング バインディング テーブルの内容を表示します。 例 19-3（P.19-8）を参照してください。
show feature	DHCP などの使用可能な機能と、それらがイネーブルかどうかを表示します。 例 19-4（P.19-8）を参照してください。
show ip arp inspection	DAI のステータスを表示します。 例 19-5（P.19-8）を参照してください。
show ip arp inspection interface vethernet *interface-number*	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。 例 19-6（P.19-9）を参照してください。
show ip arp inspection vlan *vlan-ID*	特定の VLAN の DAI 設定を表示します。 例 19-7（P.19-9）を参照してください。
show ip verify source	IP ソース ガードがイネーブルであるインターフェイスと、IP-MAC アドレス バインディングを表示します。 例 19-8（P.19-9）を参照してください。

例 19-1　show running-config dhcp

```
n1000v# show running-config dhcp

!Command: show running-config dhcp
!Time: Wed Feb 16 14:20:36 2011

version 4.2(1)SV1(4)
feature dhcp

no ip dhcp relay

n1000v#
```

例 19-2　show ip dhcp snooping

```
n1000v# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
vEthernet 3           Yes

n1000v#
```

例 19-3　show ip dhcp snooping binding

```
n1000v# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type        VLAN  Interface
------------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33  10.3.2.2         infinite  static      13    vEthernet 6
0f:00:60:b3:23:35  10.2.2.2         infinite  static      100   vEthernet 10
n1000v#
```

例 19-4　show feature

```
n1000v# show feature
Feature Name           Instance  State
--------------------   --------  --------
dhcp-snooping          1         enabled
http-server            1         enabled
ippool                 1         enabled
lacp                   1         enabled
lisp                   1         enabled
lisphelper             1         enabled
netflow                1         disabled
port-profile-roles     1         enabled
private-vlan           1         disabled
sshServer              1         enabled
tacacs                 1         enabled
telnetServer           1         enabled
n1000v#
```

例 19-5　show ip arp inspection

```
n1000v# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan : 1
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 5
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 100
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 101
-----------
Configuration          : Disabled
Operation State        : Inactive
n1000v#
```

例 19-6　show ip arp inspection interface

```
n1000v# show ip arp inspection interface vethernet 6

 Interface        Trust State
 -------------    -----------
 vEthernet 6        Trusted
n1000v#
```

例 19-7　show ip arp inspection vlan

```
n1000v# show ip arp inspection vlan 13

Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

n1000v#
```

例 19-8　show ip verify source

```
n1000v# show ip arp inspection vlan 13
IP source guard is  enabled on the following interfaces:
-------------------------------------------------------------------------------
     Vethernet1

Interface         Filter-mode     IP-address     Mac-address       Vlan
------------      -----------     ----------     --------------    ----
Vethernet11      active           25.0.0.128     00:50:56:88:00:20  25
```