



ネットワーク セキュリティの設定

この章では、Cisco 7600 シリーズ ルータ固有のネットワーク セキュリティ機能について説明します。これは、次のマニュアルに記載されているネットワーク セキュリティに関する情報および手順を補足するためのものです。

- 次の URL の『Cisco IOS Security Configuration Guide, Release 12.2』
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html
- 次の URL にある Cisco 7600 シリーズ ルータのコマンド リファレンス
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html



(注)

この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

- 次の URL の『Cisco 7600 Series Router Cisco IOS Command Reference』
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
- 次の URL にある Release 12.2 のマニュアル
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

この章の内容は、次のとおりです。

- 「MAC アドレスベースのトラフィック ブロッキングの設定」(P.35-1)
- 「TCP インターセプトの設定」(P.35-2)
- 「ユニキャスト RPF チェックの設定」(P.35-2)

MAC アドレスベースのトラフィック ブロッキングの設定

特定の VLAN 内の MAC アドレスを経由するすべてのトラフィックをブロックするには、次の作業を行います。

コマンド	目的
Router(config)# mac-address-table static <i>mac_address</i> vlan <i>vlan_ID</i> drop	特定の VLAN で設定されている MAC アドレスを経由するすべてのトラフィックをブロックします。
Router(config)# no mac-address-table static <i>mac_address</i> vlan <i>vlan_ID</i>	MAC アドレスベースのブロッキングを消去します。

次に、VLAN 12 内で MAC アドレス 0050.3e8d.6400 を経由するすべてのトラフィックをブロックする例を示します。

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

TCP インターセプトの設定

TCP インターセプト フローはハードウェアで処理されます。

設定手順については、次の URL にある『Cisco IOS Security Configuration Guide, Release 12.2』の「Traffic Filtering and Firewalls」、 「Configuring TCP Intercept (Preventing Denial-of-Service Attacks)」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfdenl.html

ユニキャスト RPF チェックの設定

ここでは、Cisco IOS ユニキャスト Reverse Path Forwarding (RPF; リバースパス転送) チェック (ユニキャスト RPF チェック) について説明します。

- 「PFC3 ユニキャスト RPF チェックのサポートの概要」 (P.35-2)
- 「ユニキャスト RPF チェックに関する注意事項および制約事項」 (P.35-3)
- 「ユニキャスト RPF チェックの設定」 (P.35-3)

PFC3 ユニキャスト RPF チェックのサポートの概要

ユニキャスト RPF チェックの機能概要の詳細については、次の URL にある『Cisco IOS Security Configuration Guide, Release 12.2』の「Other Security Features」、 「Configuring Unicast Reverse Path Forwarding」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

PFC3 は、複数のインターフェイスからのトラフィックの RPF チェックをハードウェアでサポートします。

strict 方式ユニキャスト RPF チェックの場合、PFC3 はルーティング テーブルのプレフィックスすべてに対し 2 つの平行パスと、4 つのユーザ設定変更可能な RPF インターフェイス グループ (インターフェイス グループごとに 4 つのインターフェイスを収容可能) のいずれかを通じて到達したプレフィックスに対し最大 4 つの平行パスをサポートします。

loose 方式ユニキャスト RPF チェック (別名 exist-only 方式) の場合、PFC3 は最大 8 つのリバースパス インターフェイスをサポートします (Cisco IOS ソフトウェアはルーティング テーブルでは 8 つのリバースパスに制限されます)。

Cisco IOS でユニキャスト RPF チェックを実行する方式は、次の 4 つです。

- strict ユニキャスト RPF チェック
- allow-default を使用した strict ユニキャスト RPF チェック
- loose ユニキャスト RPF チェック
- allow-default を使用した loose ユニキャスト RPF チェック

ユニキャスト RPF チェックをインターフェイス単位で設定できますが、ユニキャスト RPF チェックがイネーブルであるインターフェイスすべてに対して PFC3 がサポートするのは、ユニキャスト RPF 方式だけです。現在設定されている方式とは異なるユニキャスト RPF 方式を使用するようにインターフェイスを設定する場合、ユニキャスト RPF チェックがイネーブルになっているシステムのインターフェイスすべてが、新しい方式を使用します。

ユニキャスト RPF チェックに関する注意事項および制約事項

ユニキャスト RPF チェックの設定時には、次の注意事項および制約事項に従ってください。

- ユニキャスト RPF チェックを設定し、ACL でフィルタをかける場合、PFC はトラフィックが ACL と一致するかどうかを判断します。PFC は RPF ACL に拒否されたトラフィックを MSFC へ送信し、MSFC がユニキャスト RPF チェックを行います。ACL によって許可されたパケットは、ユニキャスト RPF チェック (CSCdz35099) を行わずにハードウェアで転送されます。
- 通常、DoS 攻撃のパケットは拒否 ACE と一致し、ユニキャスト RPF チェックを行うため MSFC に送信されます。そのため、送信されたパケットが MSFC を過負荷状態にする可能性があります。
- PFC は、ユニキャスト RPF チェックの ACL とは一致しなくても、入力セキュリティ ACL と一致するトラフィックをハードウェアでサポートします。
- PFC では、Policy-Based Routing (PBR; ポリシーベース ルーティング) トラフィックのユニキャスト RPF チェックをハードウェアでサポートしません (CSCea53554)。

ユニキャスト RPF チェックの設定

ここでは、ユニキャスト RPF チェックの設定手順について説明します。

- 「ユニキャスト RPF チェック モードの設定」(P.35-3)
- 「PFC3 での複数パスのユニキャスト RPF チェック モードの設定」(P.35-5)
- 「self-ping のイネーブル化」(P.35-6)

ユニキャスト RPF チェック モードの設定

ユニキャスト RPF には、次に示す 2 つのチェック モードがあります。

- strict チェック モード: 送信元 IP アドレスが FIB テーブルにあること、および入力ポートから到達可能な範囲内にあることを確認します。
- exist-only チェック モード: 送信元 IP アドレスが FIB テーブルにあるかどうかだけを確認します。



(注)

ユニキャスト RPF チェック用に設定されたすべてのポートには、その時点で設定されているモードが自動的に適用されます。

ユニキャスト RPF チェックの設定

ユニキャスト RPF チェック モードを設定するには、次の作業を行います。

コマンド	目的
ステップ 1 Router(config)# interface {{vlan vlan_ID} {type ¹ slot/port} {port-channel number}}	設定するインターフェイスを選択します。 (注) ユニキャスト RPF チェックは次の宛先にパケットを転送する前に、入力ポートに基づいて、最適なリターンパスを確認します。
ステップ 2 Router(config-if)# ip verify unicast source reachable-via {rx any} [allow-default] [list] Router(config-if)# no ip verify unicast	ユニキャスト RPF チェック モードを設定します。 デフォルトのユニキャスト RPF チェック モードに戻します。
ステップ 3 Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 4 Router# show mls cef ip rpf	設定を確認します。

1. *type* = ethernet、fastethernet、gigabitethernet、または tengigabitethernet

ユニキャスト RPF チェック モードを設定する際、次の情報に注意してください。

- **strict** チェック モードをイネーブルにするには、**rx** キーワードを使用します。
- **exist-only** チェック モードをイネーブルにするには、**any** キーワードを使用します。
- RPF の確認にデフォルト ルートを使用できるようにするには、**allow-default** キーワードを使用します。
- アクセス リストを識別するには、**list** オプションを使用します。
 - アクセス リストによってネットワークへのアクセスが拒否された場合は、スプーフィングされたパケットがポートで廃棄されます。
 - アクセス リストによってネットワークへのアクセスが許可された場合は、スプーフィングされたパケットが宛先アドレスに転送されます。転送されたパケットは、インターフェイスの統計情報にカウントされます。
 - アクセス リストにログ アクションが含まれている場合、スプーフィングされたパケットに関する情報がログ サーバに送信されます。



(注) **ip verify unicast source reachable-via** コマンドを入力すると、ユニキャスト RPF チェック モードがルータのすべてのポートで変更されます。

次に、ギガビット イーサネット ポート 4/1 でユニキャスト RPF の **exist-only** チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 4/2 でユニキャスト RPF の **strict** チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show running-config interface gigabitethernet 4/2
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/2
ip address 42.0.0.1 255.0.0.0
ip verify unicast reverse-path
no cdp enable
end
Router# show running-config interface gigabitethernet 4/1
Building configuration...
Current configuration : 114 bytes
!
interface GigabitEthernet4/1
ip address 41.0.0.1 255.0.0.0
→ ip verify unicast reverse-path (RPF mode on g4/1 also changed to strict-check RPF mode)
no cdp enable
end
Router#
```

PFC3 での複数パスのユニキャスト RPF チェック モードの設定

PFC3 で複数パスのユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ1	Router(config)# mls ip cef rpf mpath {punt pass interface-group} Router(config)# no mls ip cef rpf mpath {punt interface-group}	PFC3 で複数のパス RPF チェック モードを設定します。 デフォルト値に戻します (mls ip cef rpf mpath punt)。
ステップ2	Router(config)# end	コンフィギュレーション モードを終了します。
ステップ3	Router# show mls cef ip rpf	設定を確認します。

複数のパス RPF チェックを設定する場合、次の情報に注意してください。

- **punt** (デフォルト) : プレフィックスごとに最大 2 つのインターフェイスに対して、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。追加のインターフェイスに着信するパケットは MSFC3 にリダイレクト (パント) されて、ソフトウェアでユニキャスト RPF チェックが実行されます。
- **pass** : パスが 1 つまたは 2 つのプレフィックスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある **multipath** プレフィックスから着信するパケットに対し、ディセーブルです (このパケットは常にユニキャスト RPF チェックに合格します)。
- **interface-group** : パスが 1 つまたは 2 つのプレフィックスの場合、PFC3 はユニキャスト RPF チェックをハードウェアで実行します。PFC3 はプレフィックス単位で最大 4 つの追加インターフェイスに対し、ユーザ設定変更可能なマルチパス ユーザ RPF チェック インターフェイス グループを介して、ユニキャスト RPF チェックを実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある他の **multipath** プレフィックスから着信するパケットに対し、ディセーブルです (このパケットは常にユニキャスト RPF チェックが行われます)。

次に、複数パスの RPF チェックを設定する例を示します。

```
Router(config)# mls ip cef rpf mpath punt
```

PFC3 での複数パスのインターフェイス グループの設定

複数パスのユニキャスト RPF インターフェイス グループを PFC3 に設定するには、次の作業を行います。

コマンド	目的
ステップ 1 Router(config)# mls ip cef rpf interface-group [0 1 2 3] interface1 [interface2 [interface3 [interface4]]]	複数パスの RPF インターフェイス グループを PFC3 に設定します。
ステップ 2 Router(config)# mls ip cef rpf interface-group group_number	インターフェイス グループを削除します。
ステップ 3 Router(config)# end	コンフィギュレーション モードを終了します。
ステップ 4 Router# show mls cef ip rpf	設定を確認します。

次に、インターフェイス グループ 2 を設定する例を示します。

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

self-ping のイネーブル化

ユニキャスト RPF チェックがイネーブルの場合、ルータはデフォルトで self-ping を実行できません。self-ping をイネーブルにするには、次の作業を行います。

コマンド	目的
ステップ 1 Router(config)# interface {{ vlan vlan_ID } { type ¹ slot/port } { port-channel number }}	設定するインターフェイスを選択します。
ステップ 2 Router(config-if)# ip verify unicast source reachable-via any allow-self-ping Router(config-if)# no ip verify unicast source reachable-via any allow-self-ping	self-ping またはセカンダリ アドレスへの ping を実行できるように、ルータをイネーブルにします。 self-ping をディセーブルにします。
ステップ 3 Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。

1. *type* = ethernet、fastethernet、gigabithernet、または tengigabithernet

次に、self-ping をイネーブルにする例を示します。

```
Router(config)# interface gigabithernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```