ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイス上で出力トラフィックのレート制限を設定する手順について説明します。この章には次のセクションがあります。

- ユニキャスト RPF の概要, on page 1
- ユニキャスト RPF の注意事項と制約事項 （2 ページ）
- ユニキャスト RPF のデフォルト設定, on page 4
- ユニキャスト RPF の設定, on page 4
- ユニキャスト RPF の設定例, on page 6
- ユニキャスト RPF の設定の確認, on page 6

ユニキャスト RPF の概要

ユニキャスト RPF 機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IPv4 ソース アドレスが注入されて引き起こされる問題を、裏付けのない IPv4 パケットを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃では、偽造の送信元 IPv4 アドレスやすぐに変更される送信元 IPv4 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を防ぎます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF を有効にすると、スイッチはそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと発信元インターフェイスがルーティングテーブル内に現れ、しかもパケット受信場所のインターフェイスと一致することを確認します。この送信元アドレス検査は転送情報ベース（FIB）に依存しています。

Note ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるスイッチの入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、FIB のリバースルックアップを実行することにより、スイッチインターフェイスでの受信パケットがそのパケットの送信元への最良リターンパス（リターンルート）

で着信していることを確認します。パケットが最適なリバース パス ルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバース パス ルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。ユニキャストRPFがそのパケットのリバースパスを見つけられない場合は、パケットはドロップされます。

Note ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ カウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

ユニキャスト RPF

ユニキャスト Reverse Path Forwarding（RPF）機能を使用すると、ネットワークに変形または偽造（スプーフィング）された IP ソース アドレスが注入されて引き起こされる問題を、裏付けのない IP ソース アドレスを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃では、偽造の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を防ぎます。ユニキャストRPFでは、送信元アドレスが有効でIPルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

グローバル統計

Cisco NX-OS デバイスがユニキャスト RPF チェックの失敗によりインターフェイスでパケットをドロップするたびに、その情報が転送エンジン（FE）単位でデバイスにおいてグローバルにカウントされます。ドロップされたパケットのグローバル統計からは、ネットワーク上での攻撃の可能性に関する情報を得ることができますが、攻撃の送信元となるインターフェイスは特定されません。ユニキャスト RPF チェックの失敗によりドロップされたパケットのインターフェイス単位の統計情報は利用できません。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 3548 シリーズ スイッチの固有機能であるワープ モードで URPF を有効にすると、マルチキャスト エントリ数が半分になり、8 k から 4 k になります。同様に、ホスト エントリの数も、8 k の半分の 4 k になります。通常モードでは、サポートされる LPM エントリの数が半分に（24 k から 12 k に）なりますが、これは Cisco Nexus 3000 シリーズ スイッチの場合と同じです。

- ユニキャスト RPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります（ネットワークのエッジに適用するのが望ましい）。
- なるべくダウンストリームでユニキャスト RPF を適用する方が、アドレス スプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスでユニキャスト RPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバーにユニキャスト RPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソース全体でユニキャスト RPF を配布するエンティティが多いほど、インターネット コミュニティを通じた大規模なネットワークの中断が軽減される可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- ユニキャスト RPF は、総称ルーティング カプセル化（GRE）トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤ がパケットから除かれてからユニキャスト RPF がネットワーク トラフィックを処理するように、ホーム ゲートウェイにユニキャスト RPF を設定する必要があります。
- ユニキャスト RPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターン パスでもあるということです。
- ネットワーク内部のインターフェイスにはユニキャスト RPF を使用しないでください。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。ユニキャスト RPF を設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。ストリクトユニキャスト RPF を設定しないでください。
- ユニキャスト RPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラップ プロトコル（BOOTP）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

Table 1: ユニキャスト *RPF* パラメータのデフォルト設定

パラメータ	デフォルト
ユニキャスト RPF	ディセーブル

ユニキャスト RPF の設定

入力インターフェイスに次のいずれかのユニキャスト RPF モードを構成できます。

ストリクト ユニキャスト RPF モード
厳格モードでは、ユニキャスト RPF が FIB で一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると予想される場合に使用できます。

ルーズ ユニキャスト RPF モード
緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも 1 つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信した入力インターフェイスが FIB 内のインターフェイスのいずれかと一致する必要はありません。

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **hardware profile forwarding-mode warp lpm-entry** *lpm-limit* **host-entry** *host-entry-limit* **l2-entry** *l2-entry limit* **mcast-entry** *mcast-entry-limit*
3. **[no] system urpf disable**
4. **interface ethernet** *slot/port*
5. **ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
6. **exit**
7. (Optional) **show ip interface ethernet** *slot/port*
8. (Optional) **show running-config interface ethernet** *slot/port*
9. (Optional) **copy running-config startup-config**

ユニキャスト RPF の設定

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	(Optional) **hardware profile forwarding-mode warp lpm-entry** *lpm-limit* **host-entry** *host-entry-limit* **l2-entry** *l2-entry limit* **mcast-entry** *mcast-entry-limit* **Example:** `switch(config)# hardware profile forwarding-mode warp lpm-entry 4096 host-entry 4096 l2-entry 8192 mcast-entry 4096`	転送モードの lpm-entry、host-entry、および mcast-entry に指定されたカーブ値を構成します。ラップ モードの TCAM カーブ値の詳細については、を参照してください。 **Note** このコマンドは、URPF が有効になっている場合のラップ モードにのみ適用されます。
ステップ 3	**[no] system urpf disable** **Example:** `switch(config)# no system urpf disable`	スイッチでユニキャスト RPF を有効にします。 **Note** ユニキャスト RPF 構成を適用するには、Cisco NX-OS ボックスをリロードする必要があります。

ステップ 4	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 1/3`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、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 5	**ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} **Example:** `switch(config-if)# ip verify unicast source reachable-via any`	IPv4 用インターフェイスにユニキャスト RPF を設定します。 **any** キーワードは緩和モードのユニキャスト RPF を指定します。 **allow-default** キーワードを指定すると、送信元アドレスのルックアップでデフォルト ルートと一致させることが可能であり、これを検証に使用できます。 **rx** キーワードは厳格モードのユニキャスト RPF を指定します。

ステップ 6	**exit**
	Example:
	`switch(config-cmap)# exit`
	`switch(config)#`
		クラスマップ コンフィギュレーション モードを終了します。

	Command or Action	Purpose
ステップ 7	(Optional) **show ip interface ethernet** *slot/port* **Example:** `switch(config)# show ip interface ethernet 1/3`	インターフェイスの IP 情報を表示します。
ステップ 8	(Optional) **show running-config interface ethernet** *slot/port* **Example:** `switch(config)# show running-config interface ethernet 1/3`	実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 9	(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。

ユニキャスト RPF の設定例

緩和モードの IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
no system urpf disable
interface Ethernet1/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

厳格モード（ストリクト モード）の IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
no system urpf disable
interface Ethernet1/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config interface ethernet *slot/port*	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip [**all**]	実行コンフィギュレーション内の IPv4 設定を表示します。
show startup-config interface ethernet *slot/port*	スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーション内の IP 設定を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。