ユニキャスト RPF の設定

この章は、次の項で構成されています。

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、ネットワークに改変または偽造（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、検証可能な IP ソース アドレスを持たない IPv4 パケットを廃棄することにより緩和します。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）攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 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妨ぐことができます。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、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、送信元アドレスと送信元インターフェイスがルーティングテーブル内に存在しており、さらにパケット受信場所のインターフェイスとマッチ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。

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、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 プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターン パス（ルート）があるインターフェイスで受信される必要があります（このプロセスは対称ルーティングと呼ばれます）。FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。スタティック ルート、ネットワーク文、ダイナミック ルーティングによって FIB にルートが追加されます。
- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティング エントリと一致する必要があります。
- 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 エンドのデバイスの入力インターフェイスだけに適用されます。

ダウンストリーム ネットワークにインターネットへの他の接続があっても、ダウンストリーム ネットワークにユニキャスト RPF を使用できます。

Caution 攻撃者が送信元アドレスへの最良パスを変更する可能性があるので、加重やローカルプリファレンスなどのオプションの BGP 属性を使用する際には、十分に注意してください。変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

Procedure

ステップ 1 インバウンド インターフェイスで入力 ACL をチェックします。

ステップ 2 ユニキャスト RPF を使用し、FIB テーブル内のリバース ルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。

ステップ 3 パケットの転送を目的として FIB ルックアップを実行します。
ステップ 4 アウトバウンド インターフェイスで出力 ACL をチェックします。
ステップ 5 パケットを転送します。

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（uRPF）に関する注意事項と制約事項は次のとおりです。

- uRPF 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 uRPF 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 uRPF 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 サーバに uRPF 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 uRPF を展開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。
- uRPF は、汎用ルーティング 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 uRPF がネットワーク トラフィックを処理するように、uRPF はホーム ゲートウェイに設定する必要があります。
- uRPF 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。

- uRPF をネットワーク内部のインターフェイスに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。uRPF 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。厳密な uRPF を構成しないでください。
- uRPF 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。
- uRPF が有効になっている場合、IPv4 と IPv6 の両方にルーズモードが適用されます。ただし、プロトコルごとに厳密モードを適用することはできます。
- 厳密な uRPF を機能させるには、入力インターフェイスと、送信元 IP アドレスを学習したインターフェイスの両方で有効にします。
- スイッチ ハードウェアは、設定されたルーティング インターフェイスごとに厳密な uRPF を実装しません。
- 厳密な uRPF は、厳密な uRPF 対応インターフェイスの学習ルートごとに実装されます。
- ルートが ECMP として解決されると、厳密な uRPF はルーズ モードにフォールバックします。
- トラップ解決に関するハードウェアの制限により、uRPF はインバンド経由でスーパーバイザ宛パケットに適用されない場合があります。
- IP トラフィックの場合は、IPv4 と IPv6 の構成を同時に有効にするべきです。
- ハードウェアの制限により、Cisco Nexus 3600 シリーズ スイッチは次の組み合わせのみをサポートします：

uRPF の設定		**送信元 IP アドレスのトラフィックチェックの適用**		
IPv4	IPv6	IP Unipath	IP ECMP	MPLS Encap/VPN/ECMP
無効	無効	許可	許可	許可
Loose	Loose	uRPF loose	uRPF loose	uRPF loose
Strict	Strict	uRPF strict	uRPF loose	uRPF loose

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では、厳密なユニキャスト RPF モードまたは緩やかなユニキャスト RPF モードを構成できます。厳密なユニキャスト モードでは、送信元 IP がアタッチされているインターフェイスに構成を適用します。これにより、特定の送信元の許可リストを構成できます。

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。パケットを受信する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. **interface ethernet** *slot/port*
3. {**ip** | **ipv6**} **verify unicast source reachable-via any**
4. **exit**
5. (Optional) **show ip interface ethernet** *slot/port*
6. (Optional) **show running-config interface ethernet** *slot/port*
7. (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 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)#`
		イーサネットインターフェイスを指定し、インターフェイス構成モードを開始します。

ステップ 3	{**ip** | **ipv6**} **verify unicast source reachable-via any** **Example:** `switch(config-if)# ip verify unicast source reachable-via any`	IPv4 と IPv6 の両方に対するインターフェイスでユニキャスト RPF を設定します。 **Note** ユニキャスト RPF はデフォルトで無効になっているため、各インターフェイスで構成します。構成は、IPv4 と IPv6 の両方で共有されます。IPv4 と IPv6 のいずれかで有効または無効にすると、そのインターフェイス上のすべてのプロトコルに影響します。 **Note** IPv4 または IPv6 の uRPF を有効にすると（**ip** または **ipv6** キーワードを使用）、ユニキャスト RPF は IPv4 と IPv6 の両方で有効になります。 **Note** インターフェイスで使用できる IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。1 つのバージョンを設定する場合、すべてのモード変更をこのバージョンで行う必要があります。インターフェイスは、他のすべてのバージョンをブロックします。

ステップ 4	**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。

ステップ 5	(Optional) **show ip interface ethernet** *slot/port* **Example:** `switch(config)# show ip interface ethernet 2/3`	インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効かどうかを確認します。

	Command or Action	Purpose
ステップ 6	(Optional) **show running-config interface ethernet** *slot/port* **Example:** `switch(config)# show running-config interface ethernet 2/3`	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 7	(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

次に、緩和モードの IPv4/IPv6 パケット用ユニキャスト RPF の構成例を示します。

- ```
  interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
  ```

- ```
  interface Ethernet2/3
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
  ```

次に、厳密モードの IPv4/IPv6 パケット用ユニキャスト RPF の構成例を示します。

- ```
  interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
  ```

- ```
  interface Ethernet2/2
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 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。

コマンド	目的
show running-config ip6 [**all**]	実行コンフィギュレーション内の IPv6 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 ip interface ethernet *slot/port*	インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効か無効かを確認します。
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。

ユニキャスト RPF に関する追加情報

ここでは、ユニキャスト RPF の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
MPLS VPN	Cisco Nexus 3600 シリーズ NX-OS レイヤ 2 スイッチング構成ガイド

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。