ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイスで unicast reverse path forwarding（uRPF）を設定する方法を説明します。

この章は、次の項で構成されています。

ユニキャスト RPF について

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 または IPv6 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 または IPv6 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、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 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。

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。
2. ユニキャスト RFP 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。
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。
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。
5. パケットを転送します。

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、次のプラットフォームでサポートされています。
  - N9K-X9636C-R と N9K-X9636Q-R ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - N9K-X9636C-RX ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - Cisco Nexus 9300 プラットフォーム スイッチ（9300-FXP スイッチを除く）
- Cisco NX-OS リリース 9.2(1) 以降、uRPF は次でサポートされます。
  - Cisco Nexus 9300-EX シリーズ スイッチ（IPv4 のみ）
  - Cisco Nexus 9300-FX/FX2 シリーズ スイッチ（IPv4 および IPv6）
- 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にわたって uRPF を展開するエンティティ数が多くなるほど、インターネット コミュニティ全体の大規模なネットワークの中断を軽減できる可能性と、攻撃元を追跡できる可能性が高くなります。
- uRPF 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 uRPF 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 uRPF を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 は、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。
- 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 が有効な場合、スイッチがインストールできる null0 へのスタティック ルートの量は、「show hardware internal forwarding table utilization」の「Max V4 Ucast DA TCAM table entries」の値に制限されます。
- Cisco NX-OS リリース 9.2(1) 以降、N9K-X9636C-R および N9K-X96136YC-R スイッチでは、使用可能な 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。ただし、これにより、IPv4 と IPv6 の両方でユニキャスト RPF が有効になります。
- 次のガイドラインと制限は、N9K-X9636C-R、N9K-X9636C-RX、または N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチにのみ適用されます。
  - 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 アドレスが学習されたインターフェイスで有効にします。
  - 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、strict 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 の設定を同時に有効にします。
  - ハードウェアの制限により、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ライン カード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 EncapVPNECMP	N9K-X9636C-RX ライン カードの Unipath MPLS VPN
無効	無効	許可	許可	許可	許可
Loose	Loose	uRPF loose	uRPF loose	uRPF loose	uRPF strict
Strict	Strict	uRPF strict	uRPF loose	uRPF loose	uRPF strict

- Strict uRPF は、次のプラットフォームの VxLAN 経由でインターフェイスに送信される ICMP トラフィックをブロックします。
  - Cisco Nexus 9200 プラットフォーム スイッチ
  - Cisco Nexus 9300--EX/FX/GX プラットフォーム スイッチ
  - N9K-X9700-EX および N9K-X9700-FX ライン カードを搭載した Nexus 9500 スイッチ
- Strict uRPF が構成されている場合は、サブネットの背後にある未解決のホストに対して urpf strict モードが機能するように、次のコマンドを追加します。
  - **no system multicast dcs-check**
  - **hardware profile multicast max-limit lpm-entries 0**

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

-R ライン カードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定

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	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	{**ip** | **ipv6**} **address** *ip-address/length* **Example:** `switch(config-if)# ip address 172.23.231.240/23`	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 4	{**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** IPv4 または IPv6 の uRPF をイネーブルにすると（**ip** または **ipv6** キーワードを使用）、uRPF は IPv4 と IPv6 の両方でイネーブルになります。
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 情報を表示します。
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。

	Command or Action	Purpose
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。

Cisco Nexus 9300 スイッチのユニキャスト RPF の設定

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。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	[**no**] **system urpf disable** 例： `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。 （注） ユニキャスト RPF 設定を適用するには、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 3	**interface ethernet** *slot/port*
	例：
	`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 コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	{**ip** | **ipv6**} **address** *ip-address/length* 例： `switch(config-if)# ip address 172.23.231.240/23`	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 5	{**ip** | **ipv6**} **verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} 例： `switch(config-if)# ip verify unicast source reachable-via any`	IPv4 および IPv6 用インターフェイスにユニキャスト RPF を設定します。 （注） IPv4 または IPv6 のユニキャスト RPF 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。 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はこのバージョンで行う必要があり、他のすべてのバージョンはそのインターフェイスによってブロックされます。 • **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。 （注） **allow-default** キーワードは、ALPM ルーティング モードでは適用されません。 （注） **allow-default** キーワードを指定しない場合、送信元アドレス ルックアップ（ルーズなユニキャスト RPF チェックの場合）はデフォルト ルートと一致しません。 • **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。

	コマンドまたはアクション	目的

ステップ 6	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		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 7	（任意） **show ip interface ethernet** *slot/port*
	例：
	`switch(config)# show ip interface ethernet 1/54 | grep -i "unicast reverse path forwarding"`
	`IP unicast reverse path forwarding: none`
		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。

ステップ 8	（任意） **show running-config interface ethernet** *slot/port* 例： `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 9	（任意） **copy running-config startup-config** 例： `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、-R ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

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

次に、-R ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

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

次に、 Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/3
  ip address 172.23.231.240/23
```

```
  ip verify unicast source reachable-via any
```

次に、 Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

次に、 Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

次に、 Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/4
  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、次のいずれかの操作を行います。

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 running-config ipv6 [**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 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 9000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド（Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide）

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。