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。

この章は、次の内容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 機能では、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ことによって緩和します。 たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的な Denial of Service（DoS; サービス拒絶）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 をイネーブルにすると、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、かつパケットが受信された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 Forwarding Information Base（FIB; 転送情報ベース）に依存しています。

（注） 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 パスで着信す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。

（注） 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する必要があります（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。

注意 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。

手順の概要

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。
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。

手順の詳細

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。

グローバル統計情報

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Forwarding Engine（FE;転送エンジン）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 のライセンス要件

製品	ライセンス要件
Cisco NX-OS	ユニキャストRPFにはライセンスは必要ありません。 ライセンス パッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS のライセンス方式に関する詳細は、*Cisco NX-OS* ライセンス ガイドを参照してください。

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。

- 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 サーバにユニキャスト RPF を適用すると、攻撃の範囲を限定し、攻撃の送信元をトレースできますが、多くのサイトにユニキャストRPFを配布するため、ネットワーク運用の管理コストが増大します。
- 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。
- 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、Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

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。

表 *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 モードを設定できます。

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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
4. **ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
5. **exit**
6. （任意） **show ip interface ethernet** *slot*/*port*
7. （任意） **show running-config interface ethernet** *slot*/*port*
8. （任意） **copy running-config startup-config**

ユニキャスト RPF の設定

手順の詳細

	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 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*
	
	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。

ステップ 3	**ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**} 例： `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 4	**ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
	
	例：
	`Example:`
	`switch(config-if)# ipv6 verify unicast source reachable-via any`
		IPv6 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 5	**exit**
	
	例：
	`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 6	**show ip interface ethernet** *slot/port* 例： `switch(config)# show ip interface ethernet 2/3`	（任意） インターフェイスの IP 情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	**show running-config interface ethernet** *slot/port* 例： `switch(config)# show running-config interface ethernet 2/3`	（任意） 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 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

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

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

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

緩和モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

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

厳格モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

```
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。