CHAPTER 13

uRPF

シスコの総合セキュリティ システムには、広範囲に選択された機能豊富なセキュリティ サービスが組み込まれていて、法人カスタマー、企業カスタマー、およびサービス プロバイダーのカスタマーに、信頼性の高い、保護されたビジネス アプリケーションおよびサービスの導入を提案します。

攻撃防御は、総合的セキュリティ アプローチの中でも重要な側面で、未然防止策の実装に関係します。有益な攻撃防御ツールの 1 つとして、Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）があります。

uRPF の主な機能は、着信パケットのパスがローカル パケットのフォワーディング情報と一致しているかどうか確認することです。これは、着信パケットの送信元 IP アドレスを使用してそのアドレスへの現在のパス（隣接）を決定し、逆経路ルックアップ（つまり、この機能の名前）を実行することにより達成されます。このパスの検証により、uRPF がパケットを渡すか、ドロップするかが決定されます。

パスの一貫性を判別するのに使用される特定の uRPF パス検証基準は、インターフェイス上でイネーブルとなっている特定の uRPF モードにより異なります。表 13-1 に、Cisco 10000 シリーズ ルータがサポートする 2 つの uRPF モードについて示します。

表 13-1　2 つの uRPF モード

uRPF モード	パス解決テーブル	uRPF パス選択基準
ストリクト	CEF FIB	送信元 IP アドレスへのパスは、パケットが着信したのと「同じ」インターフェイスを経由している必要がある。
ルーズ	CEF FIB	送信元 IP アドレスへのパスは、デバイス上の「*任意の*」インターフェイスを経由している。

パスに応じて、パケットは次のように処理されます。

- 有効 — パケットを転送します。
- 無効 — パケットは暗黙のうちに廃棄されます。

uRPF は Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）Forwarding Information Base（FIB; 転送情報ベース）を使用して、着信パケットの送信元 IP アドレスに関して逆経路ルックアップを実行します。CEF FIB はネットワーク レイヤ ルーティング情報のデータベースで、パケットの CEF スイッチングで使用される、フォワーディング / 隣接情報に関連付けられています。CEF FIB には、すべての既知の IP プレフィクスとそれに関連付けられる隣接へのパスが入力されています。そのため、uRPF 逆経路検証において重要な要素となります。uRPF をインターフェイス上でイネーブルにすると、そのインターフェイスの入力パス上のすべての IP パケットがチェックされます。

（注）　Cisco 10000 シリーズ ルータでは、IPv4 に対しては、uRPF のストリクト モードとルーズ モードの両方をサポートしますが、IPv6 に対しては、ストリクト モードのみをサポートします。

uRPF 機能については、次の項目で説明します。

uRPF 機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(27)SBB	この機能が Cisco 10000 シリーズ ルータに導入されました（ストリクト モードのみ）。	PRE2
12.2(33)SB	Cisco 10000 上で、この機能が IPv4 トラフィック用にストリクト モードとルーズ モードの両方と統合されました。	PRE2、PRE3 および PRE4

uRPF の要件

ルータで uRPF を設定する場合は、インターフェイスで IP アドレッシングがサポートされていることを確認します。ブロードバンド インターフェイスの場合、その他すべての IP 設定とともに uRPF 設定をバーチャル テンプレートに追加する必要があります。

uRPF の制約事項

Cisco 10000 の uRPF 機能には、次の制約事項があります。

- マルチホーミングによりクライアントへの冗長サービス確立という目的が達成できなくなるため、クライアントを同一ルータにマルチホーミングしないでください。
- カスタマーは、アップリンク方向の（インターネットに流出する）パケットがリンクにアドバタイズされているルートと一致していることを確認する必要があります。そうでない場合、これらのパケットは uRPF により不正パケットとしてフィルタリングされます。
- uRPF は、CEF をサポートするプラットフォーム イメージに対してのみ使用可能です。uRPF は、Cisco IOS Release 11.1(17)CC、12.0、およびそれ以降でサポートされます。Cisco IOS Release 11.2 または 11.3 では使用できません。
- uRPF は、MPLS によってサポートされません。IP トラフィック（IPv4 と IPv6）によってのみサポートされます。ただし、IPv6 では、allow-default オプションが有効な場合に、ストリクト モードでのみ uRPF をサポートします。
- uRPF は Access Control List（ACL; アクセス コントロール リスト）をサポートしません。
- uRPF がルータ上で適切に機能するためには、CEF が必要です。CEF の詳細については、『*Cisco IOS Switching Services Configuration Guide*』を参照してください。
- デフォルトの uRPF プロビジョニングなしの urpf drop が pxf で実行されるは、次のような場合です。
  - インターフェイスがアップ状態でない。
  - インターフェイス上に IP アドレスが存在しない。

uRPF の設定

uRPF を使用するには、ルータで CEF スイッチングまたは CEF 分散スイッチングが設定されている必要があります。入力インターフェイスには、uRPF が送信元 IP アドレスを使用した FIB を介する検索機能として実装されているため、CEF スイッチングを設定する必要はありません。ルータ上で CEF が実行されている限り、個々のインターフェイスには別のスイッチング モードを設定できます。uRPF は、いずれかのタイプのカプセル化をサポートするインターフェイスまたはサブインターフェイス上で有効となる入力側の機能で、ルータに着信する IP パケット上で動作します。CEF がルータ上でグローバルにオンであることが非常に重要です。uRPF は、CEF がなければ稼働しません。

uRPF を設定するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config)# ip cef`	ルータ上で CEF をイネーブルにします。 特定のインターフェイスで CEF がサポートしない機能が設定されている場合、そのインターフェイス上で CEF をディセーブルにすることができます。CEF をグローバルにイネーブルにして特定のインターフェイスではディセーブルにするには、 **no ip route-cache cef** インターフェイス コマンドを使用できます。このコマンドにより、特定のインターフェイス以外でエクスプレス フォワーディングを使用できるようになります。特定のインターフェイスで CEF 動作をディセーブルにした後で、再びイネーブルにする場合は、インターフェイス コンフィギュレーション モードで **ip route-cache cef** コマンドを使用します。
ステップ 2	`Router(config-if)# interface` *type*	uRPF を適用する入力インターフェイスを選択します。これは、uRPF がパケットを次の宛先に転送する前に最適なリターン パスを確認できる受信インターフェイスです。 インターフェイス タイプは、ルータおよびルータにインストールされたインターフェイス カードのタイプに固有です。使用可能なインターフェイス タイプの一覧を表示するには、**interface ?** コマンドを入力します。

ステップ 3	`Router(config-if)# ip verify unicast source reachable-via any`
	or
	`Router(config-if)# ip verify unicast source reachable-via rx`
		インターフェイスで uRPF をイネーブルにします。
		
		any オプションを指定すると、ルータで Loose モード の uRPF がイネーブルになります。このモードでは、ルータは任意のインターフェイスを介して送信元アドレスに到達できます。
		
		rx オプションを指定すると、ルータで Strict モード の uRPF がイネーブルになります。このモードでは、ルータはパケットが着信したインターフェイスのみを介して送信元アドレスに到達できます。
		
		また **allow-default** オプションを使用して、送信元アドレスをチェックする場合にデフォルト ルートを照合するようにもできます。**allow-self-ping option** オプションを指定すると、ルータは自身に PING を実行することができます。

ステップ 4	`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。uRPF を適用するインターフェイスごとに、ステップ 2 およびステップ 3 を繰り返します。

（注） 通常のルーティング テーブルに存在しないすべてのアドレスに対して、デフォルト ルートを使用してデフォルト パスを設定できます。uRPF を設定する場合に allow-default オプションを使用すると、uRPF モードに応じて、有効なデフォルト パスに対して解決済みの送信元アドレスを持つ IP パケットを許可できます。ストリクト モードの uRPF では、デフォルト ルートが示すのと同じインターフェイスからのパケットは許可されます。ルーズ モードの uRPF では、デフォルト ルートに対して解決済みの送信元アドレスを持つパケットが許可されます。ただし、ルータでデフォルト ルートがプロビジョニングされていない場合は、有効なデフォルト パスが存在しないため、uRPF モードがいずれの場合でも allow-default オプションの効力はありません。

uRPF のモニタリングおよびメンテナンス

uRPF では、不正または偽造された送信元アドレスのためドロップ、あるいは圧縮されたパケット数をカウントします。uRPF は、ドロップまたは転送されたパケットで、次のグローバルな情報およびインターフェイス単位の情報を含むものをカウントします。

- グローバルな uRPF ドロップ
- インターフェイス単位の uRPF ドロップ

ルータ上で uRPF をイネーブルにすると、次のコマンドを使用して、ルータがドロップしたパケット数を監視できるようになります。

コマンド	説明
`Router# show ip traffic`	uRPF ドロップおよびドロップ抑制についてのグローバルなルータ統計情報を表示します。
`Router# show ip interface` *type*	uRPF ドロップおよびドロップ抑制についてのインターフェイス単位の統計情報を表示します。
`Router# show pxf cpu statistics drop` *interface*	uRPF プロビジョニングがない場合、およびインターフェイスがアップ状態でないか、インターフェイスに IP アドレスがない場合でも、所定のインターフェイスの pxf によるドロップ カウンタを表示します。

注意 デバッグ出力は CPU プロセスで高優先順位に割り当てられているので、システムを使用不能な状態にする可能性があります。そのため、特定の問題をトラブルシューティングする場合、またはシスコシステムズのテクニカル サポート担当者とのトラブルシューティング セッション時以外はデバッグ コマンドを使用しないようにしてください。また、ネットワーク トラフィックが低く、ユーザが少ないときにデバッグ コマンドを使用するのが最適です。このような時間にデバッグを行えば、デバッグ コマンドの増加したオーバーヘッド処理によってシステム利用に影響が及ぶ可能性が軽減されます。

例 13-1 に、**show ip traffic** コマンドを使用して、ルータ上のすべてのインターフェイスでドロップされたパケットの総数を示します。uRPF ドロップ カウントは、IP 統計情報のセクションに含まれます。

例 13-1　show ip traffic コマンド

```
Router# show ip traffic

IP statistics:
  Rcvd:  1753234 total, 1163482 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         1162010 unknown protocol, 523362 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 331512 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  15 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 5 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
```

ドロップまたは抑制されたパケットのカウントに非ゼロ値がある場合は、次のいずれかを意味します。

- パケットの送信元アドレスが不正である（通常の動作）。
- ルータは、非対称ルーティングが存在する環境（すなわち、送信元アドレスに対する最適なリターン パスとして複数のパスが存在する場合）で、uRPF を使用するように不正に設定されている。

（注） 送信元アドレスが解決されると、アドレスはスプーフィングと考えられているため、RPF カウンタは NULL 0 に増加します。

例 13-2 に、**show ip interface** コマンドを使用して、特定のインターフェイスでドロップまたは抑制されたパケットの総数を示します。

例 13-2　show ip interface コマンド

```
Router> show ip interface gigabitEthernet 8/1/0

GigabitEthernet8/1/0 is up, line protocol is up
  Internet address is 80.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP CEF turbo switching turbo vector
```

```
  Associated unicast routing topologies:
        Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: uRPF
  IP verify source reachable-via ANY
   5 verification drops
   5 suppressed verification drops
   0 verification drop-rate
```

例 13-3 に、**show pxf cpu statistics drop** *interface* コマンドを使用して、uRPF ドロップが PXF でも実行される方法を示します。

例 13-3　show pxf cpu statistics drop interface コマンド

```
router# sh pxf cpu statistics drop g8/1/0
FP drop statistics for GigabitEthernet8/1/0
                            packets            bytes
    vcci undefined          0                  0
    bad vlan id             0                  0
  vcci 9E6
    in l2 max mtu           0                  0
    in l2 min mtu           0                  0
    encap not supported     0                  0
    mlfr fragament          0                  0
    mpls not enabled        0                  0
    ip version              0                  0
    ip header length        0                  0
    ip length max           0                  0
    ip length min           0                  0
    ip checksum             0                  0
    fib rpf fail            0                  0
    acl denied              0                  0
    ttl                     0                  0
    unreachable             0                  0
    df multicast            0                  0
    police input drop       0                  0
    police output drop      0                  0
    out l2 max mtu          0                  0
    out l2 min mtu          0                  0
    tunnel no match         0                  0
    iedge input drop(s)     0                  0
    iedge output drop(s)    0                  0
```

uRPF の設定例

ここでは、次の設定例を示します。

- ルーズ モードの uRPF の設定
- allow-self-ping オプションによるルーズ モードの uRPF の設定
- allow-default オプションによるルーズ モードの uRPF の設定

ルーズ モードの uRPF の設定

例 13-4 に、ルータのギガビット イーサネット インターフェイス上でルーズ モードの uRPF をイネーブルする例を示します。

例 13-4　8/1/0 インターフェイスでのルーズ モードの uRPF の設定

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# int g8/1/0
Router (config-if)# ip verify unicast source reachable-via?
  any Source is reachable via any interface
  rx   Source is reachable via interface on which packet was received

Router (config-if)# ip verify unicast source reachable-via any?
  <1-199>          IP access list (standard or extended)
  <1300-2699>      IP expanded access list (standard or extended)
  allow-default    Allow default route to match when checking source address
  allow-self-ping  Allow router to ping itself (opens vulnerability in
                   verification)
  <cr>

Router (config-if)# ip verify unicast source reachable-via any
Router (config-if)# end
```

例 13-5 に、**show router interface** コマンドを使用して、ルータ上でルーズ モードの uRPF が設定されていることを確認する例を示します。

例 13-5　8/1/0 インターフェイスでのルーズ モードの uRPF の確認

```
Router# sh ru interface gig8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any
 negotiation auto
end
```

allow-self-ping オプションによるルーズ モードの uRPF の設定

例 13-6 に、**allow-self-ping** オプションを使用してルーズ モードの uRPF を設定する例を示します。

例 13-6　allow-self-ping オプションによるルーズ モードの uRPF

```
Router(config)# int g8/1/0
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
Router# sh ru int g8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any allow-self-ping
 negotiation auto
end
```

（注）　allow-self ping オプションを使用して uRPF をインターフェイスでイネーブルにした後、self-ping オプションが有効かどうか確認するため、自身への PING を開始します。

allow-default オプションによるルーズ モードの uRPF の設定

例 13-7 に、**allow-default** オプションを使用してルーズ モードの uRPF を設定する例を示します。

例 13-7　allow-default オプションによるルーズ モードの uRPF

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int g8/1/0
Router(config-if)# ip verify unicast source reachable-via any allow-default
Router(config-if)# end
Router# sh ru int gig8/1/0
!
interface GigabitEthernet8/1/0
 ip address 80.1.1.1 255.255.255.0
 ip verify unicast source reachable-via any allow-default
 negotiation auto
end
```

（注）　ストリクト モードの uRPF を設定する場合は、**ip verify unicast source reachable-via** コマンドの、**any** キーワードを **rx** に置き換えます。