

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ASR9000 での送信元ベースの RTBH フィルタリング](#)

[設定](#)

[トリガー ルータでの設定](#)

[境界ルータでの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、アグリゲーション サービス ルータ (ASR) 9000 で Remotely Triggered Blackhole (RTBH) を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS-XR[®] および ASR 9000 に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

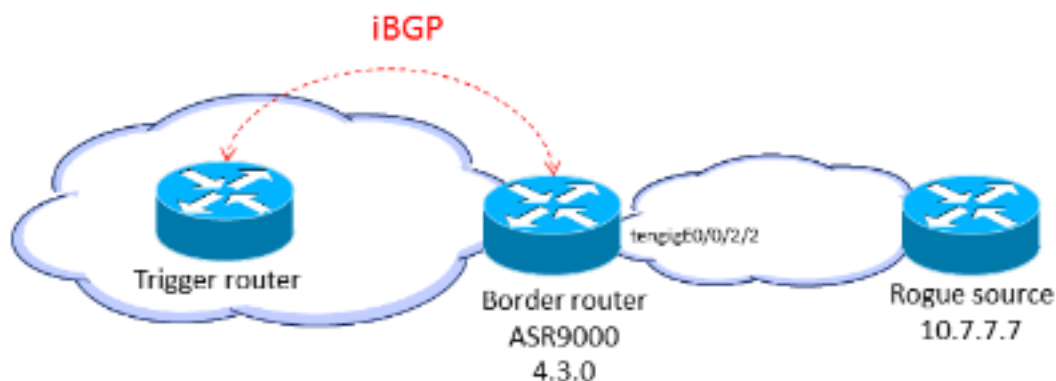
攻撃元が判明している場合 (たとえば、NetFlow データの分析によって)、アクセス コントロール リスト (ACL) などの抑制メカニズムを適用できます。攻撃のトラフィックが検出されて分類されると、該当する ACL を作成して必要なルータに展開できます。この手動プロセスは時間が

かかる上に、複雑になる可能性があるため、多くのユーザは Border Gateway Protocol (BGP) を使用して、破棄情報をすべてのルータに迅速かつ効率的に伝搬します。この RTBH という手法では、攻撃対象の IP アドレスのネクスト ホップを null インターフェイスに設定します。攻撃対象が宛先のトラフィックは、ネットワークへの進入時に破棄されます。

別のオプションは、特定の送信元からのトラフィックの破棄です。この方法は、前述の破棄と似ていますが、パケットの送信元が「invalid」(無効)(これには、null0 へのルートが含まれている)の場合、パケットを破棄する、Unicast Reverse Path Forwarding (uRPF) の以前の展開に依存します。宛先ベースの破棄と同じメカニズムを使用して、BGP 更新が送信され、この更新により送信元のネクスト ホップが null0 に設定されます。これで、uRPF が有効になったインターフェイスに入るすべてのトラフィックによって、その送信元からのトラフィックが破棄されます。

ASR9000 での送信元ベースの RTBH フィルタリング

uRPF 機能を ASR9000 で有効にすると、ルータでは null0 に対する再帰ルックアップを実行できません。これは、Cisco IOS によって使用される送信元ベースの RTBH フィルタリング設定が、ASR9000 上の Cisco IOS-XR によっては直接使用できないことを意味しています。代替手段として、ルーティング ポリシー言語 (RPL) の `set next-hop discard` オプション (Cisco IOS XR バージョン 4.3.0 で導入された) を使用します。



設定

トリガー ルータでの設定

次に示すようにして、特殊なタグでマークされたスタティック ルートにコミュニティを設定する、スタティック ルート再配布ポリシーを設定して、それを BGP で適用します。

次に示すようにして、ブラックホール化する必要がある送信元プレフィックスに特殊なタグの付いたスタティック ルートを設定します。

境界ルータでの設定

次に示すようにして、トリガー ルータに設定されたコミュニティに一致するルート ポリシーを設定し、`set next-hop discard` を設定します。

次に示すようにして、iBGP ピアにルート ポリシーを適用します。

次に示すようにして、境界インターフェイスに、uRPF ルーズ モードを設定します。

注 この uRPF 設定は、このインターフェイス上のすべてのトラフィックに適用されます。

確認

次に示すように、境界ルータでは、プレフィックス 10.7.7.7/32 に Nexthop-discard とフラグが付きます。

```
RP/0/RSP0/CPU0:router#show bgp
BGP router identifier 10.210.0.5, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000 RD version: 12
BGP main routing table version 12
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
N>i10.7.7.7/32          192.168.102.2          0      100      0 ?

RP/0/RSP0/CPU0:router#show bgp 10.7.7.7/32
BGP routing table entry for 10.7.7.7/32
Versions:
Process bRIB/RIB SendTblVer
Speaker 12 12
Last Modified: Jul 4 14:37:29.048 for 00:20:52
Paths: (1 available, best #1, not advertised to EBGp peer)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
192.168.102.2 (discarded) from 192.168.102.2 (10.210.0.2)
Origin incomplete, metric 0, localpref 100, valid, internal best, group-best
Received Path ID 0, Local Path ID 1, version 12
Community: 1234:4321 no-export
```

```
RP/0/RSP0/CPU0:router#show route 10.7.7.7/32

Routing entry for 10.7.7.7/32
  Known via "bgp 65001", distance 200, metric 0, type internal
  Installed Jul 4 14:37:29.394 for 01:47:02
  Routing Descriptor Blocks
    directly connected, via Null0
      Route metric is 0
  No advertising protos.
```

RPF 廃棄が発生していることは入力ラインカードで検証できます。

```
RP/0/RSP0/CPU0:router#show cef drop location 0/0/CPU0
CEF Drop Statistics
Node: 0/0/CPU0
Unresolved drops packets : 0
Unsupported drops packets : 0
```

```
Null0 drops packets : 10
No route drops packets : 17
No Adjacency drops packets : 0
Checksum error drops packets : 0
RPF drops           packets :          48505   <=====
RPF suppressed drops packets : 0
RP destined drops packets : 0
Discard drops packets : 37
GRE lookup drops packets : 0
GRE processing drops packets : 0
LISP punt drops packets : 0
LISP encap err drops packets : 0
LISP decap err drops packets :
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [REMOTELY TRIGGERED BLACKHOLE フィルタリング - 宛先ベースおよび送信元ベース](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)