RPL のネクストホップ廃棄と ASR9000 送信元ベースでリモートからトリガーされるブラックホール フィルタリングの設定例

内容

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特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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

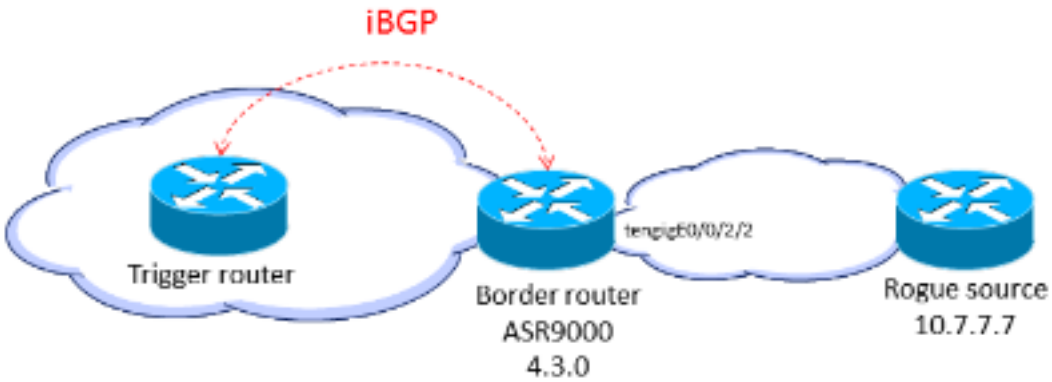
背景説明

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。

```
route-policy RTBH-trigger
if tag is 777 then
```

```
set community (1234:4321, no-export) additive
pass
else
pass
endif
end-policy

router bgp 65001
address-family ipv4 unicast
redistribute static route-policy RTBH-trigger
!
neighbor 192.168.102.1
remote-as 65001
address-family ipv4 unicast
route-policy bgp_all in
route-policy bgp_all out
```

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。

```
router static
address-family ipv4 unicast
10.7.7.7/32 Null0 tag 777
```

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。

```
route-policy RTBH
if community matches-any (1234:4321) then
set next-hop discard
else
pass
endif
end-policy
```

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。

```
router bgp 65001
address-family ipv4 unicast
!
neighbor 192.168.102.2
remote-as 65001
address-family ipv4 unicast
route-policy RTBH in
route-policy bgp_all out
```

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。

```
interface TenGigE0/0/2/2
cdp

ipv4 address 192.168.101.2 255.255.255.0
ipv4 verify unicast source reachable-via any
```

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 :
```

トラブルシュート

現在、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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。