Exemplo de Configuração de Filtragem de Blackhole Acionada Remotamente com Base na Origem ASR9000 com Descarte de Próximo Salto RPL

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Filtragem RTBH baseada em origem no ASR9000](#)
[Configurar](#)
[Configuração no Roteador de Disparo](#)
[Configuração no roteador de borda](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o Remote Triggered Blackhole (RTBH) no Aggregation Services Router (ASR) 9000.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Essas informações neste documento são baseadas no Cisco IOS-XR® e ASR 9000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

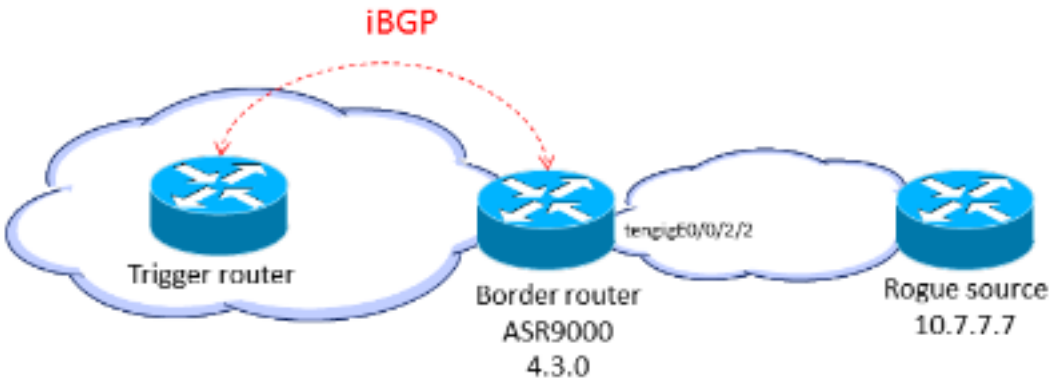
Informações de Apoio

Quando você souber a origem de um ataque (por exemplo, por meio de uma análise dos dados do NetFlow), poderá aplicar mecanismos de contenção, como Listas de Controle de Acesso (ACLs). Quando o tráfego de ataque é detectado e classificado, você pode criar e implantar ACLs apropriadas nos roteadores necessários. Como esse processo manual pode ser demorado e complexo, muitas pessoas usam o Border Gateway Protocol (BGP) para propagar informações de descarte para todos os roteadores de forma rápida e eficiente. Essa técnica, RTBH, define o próximo salto do endereço IP da vítima para a interface nula. O tráfego destinado à vítima é descartado no ingresso na rede.

Outra opção é descartar o tráfego de uma origem específica. Esse método é semelhante ao descarte descrito anteriormente, mas depende da implantação anterior do Unicast Reverse Path Forwarding (uRPF), que descarta um pacote se sua origem for "inválida", o que inclui rotas para null0. Com o mesmo mecanismo de queda baseada no destino, uma atualização de BGP é enviada e esta atualização define o próximo salto para uma origem como null0. Agora todo o tráfego que entra em uma interface com uRPF habilitado descarta o tráfego dessa origem.

Filtragem RTBH baseada em origem no ASR9000

Quando o recurso uRPF está habilitado no ASR9000, o roteador não consegue fazer uma pesquisa recursiva em null0. Isso significa que a configuração de filtragem RTBH baseada em origem usada pelo Cisco IOS não pode ser usada diretamente pelo Cisco IOS-XR no ASR9000. Como alternativa, a opção **set next-hop discard** do Routing Policy Language (RPL) (apresentada no Cisco IOS XR versão 4.3.0) é usada.



Configurar

Configuração no Roteador de Disparo

Configure uma política de redistribuição de rota estática que defina uma comunidade em rotas estáticas marcadas com uma marca especial e aplique-a no BGP:

```
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
```

Configure uma rota estática com a marca especial para o prefixo de origem que precisa ser black-holed:

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

Configuração no roteador de borda

Configure uma política de rota que corresponda à comunidade definida no roteador acionador e configure **set next-hop discard**:

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

Aplique a política de rota nos peers do iBGP:

```
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
```

Nas interfaces de borda, configure o modo solto uRPF:

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

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

Observação: essa configuração uRPF se aplica a todo o tráfego nessa interface.

Verificar

No roteador de borda, o prefixo **10.7.7.7/32** é sinalizado como **Nexthop-discard**:

```
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.
```

Você pode verificar nas placas de linha de ingresso que ocorrem descartes de RPF:

```
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 :
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- FILTRAGEM DE BURACO NEGRO DISPARADA REMOTAMENTE - COM BASE NO DESTINO E NA ORIGEM
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.