ASR9000 Blackhole remotamente provocado com base na origem que filtra com exemplo de configuração do descarte do salto seguinte RPL

Índice

Introdução

Este documento descreve como configurar Blackhole remotamente provocado (RTBH) no roteador dos serviços da agregação (ASR) 9000.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Esta informação neste documento é baseada no ® do Cisco IOS XR e no ASR 9000.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Quando você conhecer a origem de um ataque (por exemplo, por uma análise dos dados de Netflow), você pode aplicar mecanismos da retenção, tais como o Access Control Lists (ACLs). Quando o tráfego do ataque é detectado e classificado, você pode criar e distribuir ACL apropriados ao Roteadores necessário. Porque este processo manual pode ser demorado e complexo, muitos povos usam o Border Gateway Protocol (BGP) a fim propagar rapidamente e eficientemente a informação da gota a todo o Roteadores. Esta técnica, RTBH, ajusta o salto seguinte do endereço IP de Um ou Mais Servidores Cisco ICM NT da vítima à interface nula. O tráfego destinado à vítima é deixado cair no ingresso na rede.

Uma outra opção é deixar cair o tráfego de um origem específica. Este método é similar à gota descrita previamente mas confia no desenvolvimento precedente do Unicast Reverse Path Forwarding (uRPF), que deixa cair um pacote se sua fonte é “inválida,” que inclui rotas ao null0. Com o mesmo mecanismo da gota destino-baseada, uma atualização BGP é enviada, e esta atualização ajusta o salto seguinte para uma fonte ao null0. Agora todo o tráfego que incorpora uma relação com uRPF permitiu o tráfego das gotas dessa fonte.

RTBH com base na origem que filtra no ASR9000

Quando o uRPF da característica é permitido no ASR9000, o roteador é incapaz de fazer a consulta recursivo ao null0. Isto significa que a configuração de filtração com base na origem RTBH usada pelo Cisco IOS não pode diretamente ser usada pelo Cisco IOS XR no ASR9000. Como uma alternativa, a língua da política de roteamento (RPL) **ajustou a** opção do **descarte do salto seguinte** (introduzida na versão 4.3.0 do Cisco IOS XR) é usada.

Configurar

Configuração no roteador do disparador

Configurar uma política de redistribuição da rota estática que ajuste uma comunidade nas rotas estáticas identificadas por meio de uma etiqueta 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
```

Configurar uma rota estática com a etiqueta especial para o prefixo da fonte que precisa preto-de ser furado:

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

Configuração no roteador de borda

Configurar uma política da rota que combine o conjunto da comunidade no roteador do disparador e configurar **descarte ajustado do salto seguinte**:

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

Aplique a política da rota nos pares 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 relações da beira, configurar o modo fraco do uRPF:

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

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

> Nota: Esta configuração do uRPF aplica-se a todo o tráfego nesta relação.

Verificar

No roteador de borda, o prefixo 10.7.7.7/32 é embandeirado como o Nexthop-descarte:

```
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 do ingresso que as gotas RPF ocorrem:

```
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 :
```

Troubleshooting

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

Informações Relacionadas

- FILTRAÇÃO REMOTAMENTE PROVOCADA DO BURACO NEGRO - DESTINO BASEADO E FONTE BASEADA
- Suporte Técnico e Documentação - Cisco Systems