Esempio di configurazione di ASR9000 Source-based Blackhole Filtering attivato in remoto con RPL Next-hop Discard

Sommario

Introduzione

Questo documento descrive come configurare Remote Triggered Blackhole (RTBH) su Aggregation Services Router (ASR) 9000.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco IOS-XR® e ASR 9000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si conosce l'origine di un attacco (ad esempio, analizzando i dati NetFlow), è possibile applicare meccanismi di contenimento, quali gli Access Control Lists (ACL). Quando il traffico di attacco viene rilevato e classificato, è possibile creare e distribuire gli ACL appropriati ai router necessari. Poiché questo processo manuale può essere lungo e complesso, molte persone utilizzano il Border Gateway Protocol (BGP) per propagare le informazioni di rilascio a tutti i router in modo rapido ed efficiente. Questa tecnica, RTBH, imposta l'hop successivo dell'indirizzo IP della vittima sull'interfaccia null. Il traffico diretto alla vittima viene interrotto all'ingresso nella rete.

Un'altra opzione è quella di eliminare il traffico proveniente da una determinata origine. Questo metodo è simile al drop descritto in precedenza, ma si basa sulla precedente distribuzione di Unicast Reverse Path Forwarding (uRPF), che scarta un pacchetto se la sua origine è "non valida", che include route per null0. Con lo stesso meccanismo del drop basato sulla destinazione, viene inviato un aggiornamento BGP e questo aggiornamento imposta l'hop successivo per un'origine su null0. Ora tutto il traffico che entra in un'interfaccia con uRPF abilitato scarta il traffico da quella sorgente.

Filtraggio RTBH all'origine su ASR9000

Quando la funzione uRPF è abilitata su ASR9000, il router non è in grado di eseguire una ricerca ricorsiva su null0. Ciò significa che la configurazione del filtro RTBH basato sull'origine utilizzata da Cisco IOS non può essere utilizzata direttamente da Cisco IOS-XR su ASR9000. In alternativa, viene usata l'opzione RPL (Routing Policy Language) che consente di **impostare l'eliminazione dell'hop successivo** (introdotta in Cisco IOS XR versione 4.3.0).

Configurazione

Configurazione sul router di attivazione

Configurare un criterio di ridistribuzione delle route statiche che imposta una community sulle route statiche contrassegnate con un tag speciale e applicarlo in 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
```

Configurare una route statica con il tag speciale per il prefisso di origine che deve essere bucato in nero:

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

Configurazione sul router di confine

Configurare un criterio di route che corrisponda alla community impostata sul router di trigger e configurare l'**eliminazione dell'hop successivo impostato**:

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

Applicare la policy delle route sui peer 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
```

Sulle interfacce dei bordi, configurare la modalità uRPF loose:

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

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

Nota: questa configurazione uRPF si applica a tutto il traffico su questa interfaccia.

Verifica

Sul router di confine, il prefisso **10.7.7.7/32** è contrassegnato come **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.
```

Èpossibile verificare sulle schede di linea in entrata che si verifichino perdite 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 :
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- FILTRAGGIO DEL BUCO NERO ATTIVATO IN REMOTO - BASATO SULLA DESTINAZIONE E SULL'ORIGINE
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).