

Blackhole en Mikrotik ROS v7

Configuración de Blackhole en Mikrotik ROS v7

La siguiente es una configuración para el mecanismo de blackhole de bgp en RouterOS v7 y teniendo 2 objetivos:

Publicar una IP nuestra que está siendo atacada.

Cabase soporte que se publiquen 2 tipos de prefijos en blackhole "/32" y "/24", por lo tanto lo que hacemos primero es publicar en nuestro router en la tabla de ruteo principal el IP o red a bloquear y que sea del tipo blackhole.

Dir_ip_host : Dirección ip tipo x.x.x.x de nuestro host que está siendo atacado.

Dir_ip_net : Dirección ip tipo x.x.x.x de nuestra red /24 que está siendo atacada.

```
/ip route add blackhole disabled=no dst-address=Dir_ip_host/32
```

```
/ip route add blackhole disabled=no dst-address=Dir_ip_net/24
```

Definimos las propiedades de la comunidad blackhole

Ya con las rutas publicadas de forma estática en nuestra tabla de ruteo, podemos anunciarlas por BGP a nuestros peers como blackhole. Para esto vamos a definir la comunidad blackhole

```
/routing filter community-list add communities=52376:666 disabled=no list=CABASE-Blackhole
```

Creamos el filtro para ser aplicado a los anuncios de nuestro BGP

El paso siguiente es realizar una regla que aplicaremos a los anuncios de nuestro BGP teniendo en consideración que :

- Hemos instalado la ruta estatica en la tabla principal como tipo blackhole.
- Podemos anunciar a Cabase rutas /32 y /24 solamente.

```
/routing filter rule add chain=CABASE-Anuncio disabled=no rule="if ( blackhole && (dst-len == 32 || dst-len == 24 )) { append bgp-communities CABASE-Blackhole }"
```

Nota: En ROS v7 es mas facil realizar los filtros desde CLI ya que tiene la herramienta de autocompletado que es de ayuda en la edición.

Aplicamos el filtro a los anuncios de nuestro BGP

El siguiente paso es impactar la configuración en nuestra configuración de BGP teniendo en cuenta las siguiente variables que adaptan la configuración BGP:

as_local : Número de mi sistema autonomo

as_remoto : Número de sistema autonomo con el que realizo la conexión BGP (SA del IXP)

Nom_Template : Nombre que le asigno al template de configuración

Nom_BGP : Nombre de le asigno a la sesión de BGP

IP_remoto : Dirección IP contra la cual establezco la conexión BGP (IP del router del IXP).

Router-ID : Utilización de IP local para la id de router.

```
/routing bgp template add as=as_local disabled=no name=Nom_Template
```

```
/routing bgp connection add as=as_local disabled=no local.role=ebgp name=Nom_BGP  
output.filter-chain=CABASE-Anuncio .redistribute=connected,static remote.address=  
IP_remoto .as=as_remoto router-id=Router-ID routing-table=main templates=  
Nom_Template
```

Es importante aclarar que estoy anunciando las redes que tengo conectadas y las rutas que he incorporado de forma estática ".redistribute=connected,static".

Ya configurado el mecanismo de blackhole y los anuncios por BGP, solo queda incorporar los ips de hosts o redes que estan siendo atacadas como definimos en "Publicar una IP nuestra que está siendo atacada". Cuando consideremos que el ataque ha cesado, la eliminamos de la tabla de ruteo y automaticamente el el BGP la dejará de anunciar esa ruta con la comunidad blackhole permitiendo nuevamente la conectividad con el hosto o red.

Configurando nuestro router para filtrado de anuncios tipo blackhole

No menos importante que el paso anterior es el de configurar que nuestro router realice el filtrado de una ruta tipo blackhole, ya que uno de de nuestros IPs puede ser que esté atacando a la ruta (host o red) que recibimos como tipo blackhole.

Teniendo en consideración que ya está definida la comunidad blackhole para CABASE como realizamos en el paso "Definimos las propiedades de la comunidad blackhole".

Definimos el filtro de las rutas que recibimos por BGP

En nuestro router definimos que las rutas que recibimos con la comunidad blackhole de cabase la debemos incorporar a la tabla principal de ruto como tipo blackhole(null o descartar paquetes a ese destino). El siguiente filtro configura cualquier ruta que venga con la comunidad seteada "*:666"

```
/routing filter rule add chain=CABASE-Recibo disabled=no rule="if ( ( not bgp-communities-empty && bgp-communities any-regexp :666$ ) && (dst-len == 32 || dst-len == 24 )) { set blackhole yes }"
```

Aplicamos el filtro a las rutas que recibimos en nuestro BGP

El siguiente paso es impactar los filtros en nuestra configuración de BGP teniendo en cuenta las siguiente variables que adaptan la configuración BGP y la configuración del filtro de anuncio realizado anteriormente:

as_local : Número de mi sistema autonomo

as_remoto : Número de sistema autonomo con el que realizo la conexión BGP (SA del IXP)

Nom_Template : Nombre que le asigno al template de configuración

Nom_BGP : Nombre de le asigno a la sesión de BGP

IP_remoto : Dirección IP contra la cual establezco la conexión BGP (IP del router del IXP).

Router-ID : Utilización de IP local para la id de router.

```
/routing bgp template add as=as_local disabled=no name=Nom_Template
```

```
/routing bgp connection add as=as_local disabled=no input.filter=CABASE-Recibo  
local.role=ebgp name=Nom_BGP output.filter-chain=CABASE-Anuncio  
.redistribute=connected,static remote.address=IP_remoto .as=as_remoto router-id=  
Router-ID routing-table=main templates=Nom_Template
```

Revision #3

Created 8 May 2024 13:07:59 by wiki

Updated 8 May 2024 13:11:11 by wiki