

REFLEXIVE ACCESS-LISTS

Introducción. Las *reflexive access-lists*, son listas que puede utilizarse en filtros basados en información de capas superiores del modelo OSI. Esto permite establecer un tipo de filtrado en el que sólo se permita todo aquel tráfico que haya sido generado localmente.

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_ip_filter_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Topología.



Objetivo.

En la topología mostrada, se requiere que tráfico de ICMP así como de TCP sea permitido cuando la sesión se establezca originalmente desde la red 50.50.50.0/24. Cualquier tráfico generado fuera de esta red debe ser bloqueado.

Modo de Operación.

La forma en la que esta función opera es la siguiente:

1. Se requiere aplicar dos filtros en el router.
2. El primer filtro va a registrar las sesiones de ICMP y TCP generadas localmente. Dichas sesiones se van a “reflejar” en el segundo filtro.
3. El segundo filtro debe “evaluar” las sesiones capturadas por el primer filtro, permitir las y, finalmente, filtrar cualquier otro tráfico.

Configuración del router.

- Configure la lista de acceso que definirá el tráfico que nos interesa reflejar, para este ejemplo es todo el tráfico TCP e ICMP, pero puede ser tan específico como se requiera. Para utilizar esta función se requieren listas de acceso *nombradas*, ya que son las que soportan los comandos especiales para “reflejar” y “evaluar”:

```
ip access-list extended INBOUND  
permit tcp any any reflect TRAFFIC  
permit icmp any any reflect TRAFFIC
```

- La configuración anterior le indica al router que inspeccione todas las sesiones de ICMP y TCP y las registre en una lista de acceso dinámica llamada “TRAFFIC”. Como opción, después de reflejar el tráfico se puede agregar un tiempo máximo de espera que duraría una entrada dinámica sin utilizarse.
- Como siguiente paso se configura el filtro que va a evaluar la lista de acceso dinámica generada por la lista anterior.

```
ip access-list extended FILTER  
permit eigrp any any  
evaluate TRAFFIC  
deny ip any any log
```

- En la lista anterior se observa cómo permitimos la comunicación de un protocolo de ruteo, después evaluamos las entradas dinámicas de la lista TRAFFIC (reflejada desde la lista INBOUND) y finalmente agregamos un “log” a todo el tráfico no permitido para comprobar que la lista está funcionando.
- Finalmente se aplican las listas de acceso. Para este ejemplo se aplicarán como *inbound* en la interfaz LAN (INBOUND) y la interfaz WAN (FILTER).

```
interface FastEthernet0/0  
ip access-group INBOUND in  
  
interface FastEthernet1/0  
ip access-group FILTER in
```

- Después de aplicadas, la lista INBOUND registrará y reflejará cualquier sesión ICMP ó TCP originada en la LAN. Una vez reflejadas las sesiones, la lista FILTER agregará dicha información para permitir las a la entrada de la WAN. En tiempo real, se puede revisar las entradas que se agregan a la lista dinámica TRAFFIC con el comando “show access-list TRAFFIC”.

sh access-list INBOUND

Extended IP access list INBOUND

10 permit tcp any any reflect TRAFFIC (93 matches)

20 permit icmp any any reflect TRAFFIC (7 matches)

sh access-list TRAFFIC

Reflexive IP access list TRAFFIC

permit tcp host 7.7.7.7 eq telnet host 50.50.50.50 eq 11007 (100 matches) (time left 297)

permit icmp host 7.7.7.7 host 50.50.50.50 (10 matches) (time left 200)

sh access-list FILTER

Extended IP access list FILTER

10 permit eigrp any any (315 matches)

20 evaluate TRAFFIC

30 deny ip any any log (6 matches)