# GSR: Listas de control de acceso de recepción

## Contenido



## Introducción

Este documento describe una nueva función de seguridad llamada listas de control de acceso (rACLs)1 y presenta recomendaciones y pautas para los despliegues de rACL. Las ACL de recepción se utilizan para aumentar la seguridad en los routers Cisco 12000 al proteger el Gigabit Route Processor (GRP) del router contra el tráfico innecesario y potencialmente nefario. Los ACL de recepción se agregaron como exención especial para el acelerador de mantenimiento para la versión 12.0.21S2 de Cisco IOS ® Software y se integraron en la versión 12.0(22)S de Cisco IOS Software.

## Protección GRP

Los datos recibidos por un router de switch gigabit (GSR) se pueden dividir en dos grandes categorías:

- Tráfico que pasa a través del router a través de la trayectoria de reenvío.
- Tráfico que se debe enviar a través de la ruta de recepción al GRP para un análisis más detallado.

En las operaciones normales, la gran mayoría del tráfico simplemente fluye a través de un GSR en ruta a otros destinos. Sin embargo, el GRP debe manejar ciertos tipos de datos, principalmente protocolos de ruteo, acceso de router remoto y tráfico de administración de red (como el protocolo simple de administración de red [SNMP]). Además de este tráfico, otros paquetes de Capa 3 podrían requerir la flexibilidad de procesamiento del GRP. Estos incluirían ciertas opciones IP y ciertas formas de paquetes ICMP (Internet Control Message Protocol). Refiérase al apéndice sobre recibir adyacencias y paquetes punteados para obtener detalles

adicionales con respecto a las rACL y el tráfico de trayecto de recepción en el GSR.

Un GSR tiene varias rutas de datos, cada una de las cuales presta servicio a diferentes formas de tráfico. El tráfico de transición se reenvía desde la tarjeta de línea de ingreso (LC) hacia el entramado y luego hacia la tarjeta de egreso para realizar la siguiente entrega de salto. Además de la trayectoria de datos del tráfico de tránsito, un GSR tiene otras dos rutas para el tráfico que requieren procesamiento local: CPU de LC a LC y CPU de LC a LC a fabric a GRP. La tabla que se muestra a continuación ilustra los trayectos para las características y los protocolos generalmente utilizados.

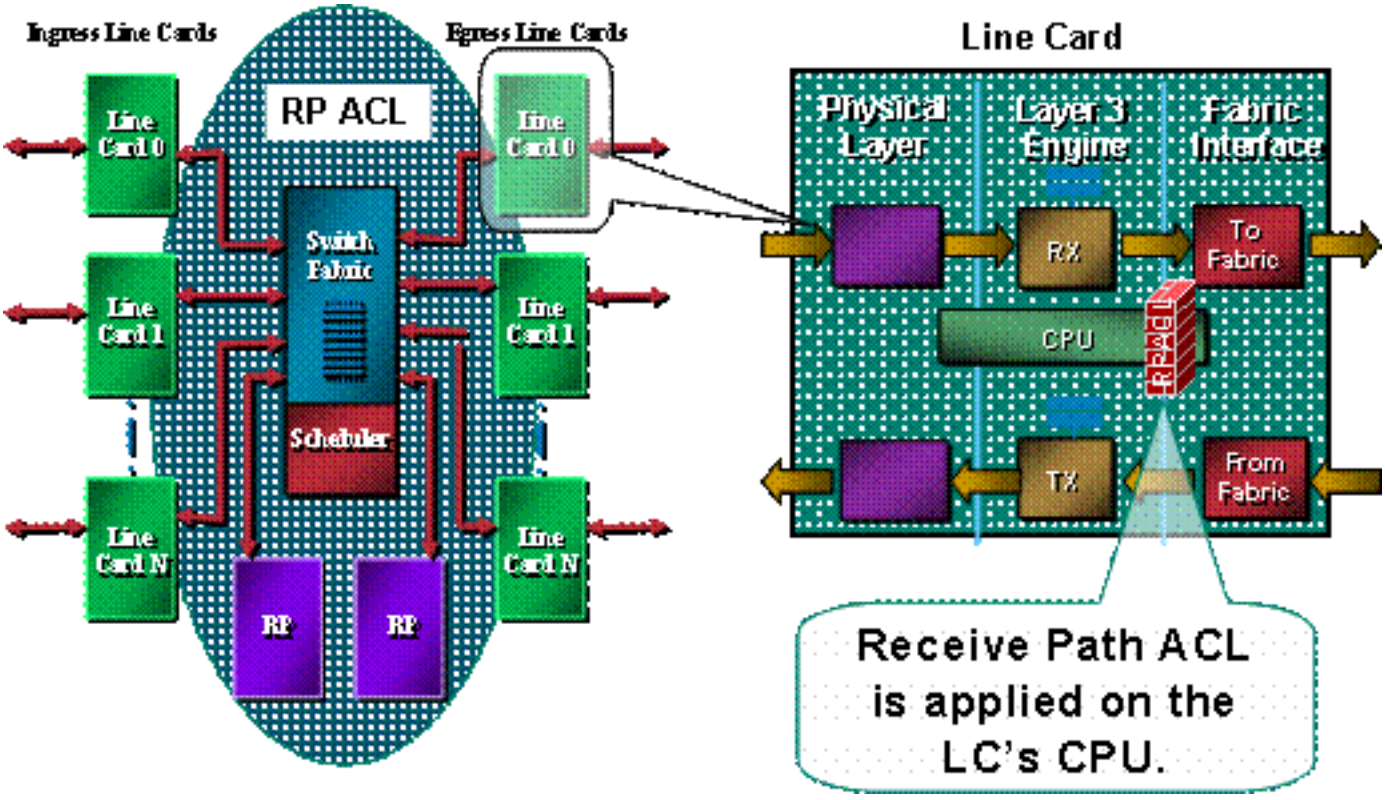
| 'Tipo de tráfico' | Ruta de datos |
|---|---|
| Tráfico normal (de tránsito) | LC a fabric a LC |
| Protocolos de routing/SSH/SNMP | CPU de LC a LC a fabric a GRP |
| Eco ICMP (ping) | CPU de LC a LC |
| Registro | |

El procesador de la ruta para el GSR tiene una capacidad limitada para procesar el tráfico enviado desde las LC y que está destinado para el GRP en sí. Si un gran volumen de datos requiere puntar al GRP, ese tráfico puede superar al GRP. Esto da lugar a un ataque de denegación de servicio (DoS) efectivo. La CPU del GRP se esfuerza por mantenerse al día con el examen de paquetes y comienza a descartar paquetes, inundando las colas de retención de entrada y descarte selectivo de paquetes (SPD). [2] Los GSR deben estar protegidos frente a tres escenarios, que pueden resultar de ataques de DoS dirigidos a un GRP del router.

- Pérdida de paquetes del protocolo de ruteo de una inundación de prioridad normal
- Sesión de administración (Telnet, Secure Shell [SSH], SNMP) pérdida de paquetes a causa de una inundación de prioridad normal
- Pérdida de paquete de una inundación de alta prioridad simulada

La pérdida potencial de los datos del protocolo de ruteo durante una inundación de prioridad normal actualmente se ve aliviada por la clasificación estática y el límite de velocidad del tráfico destinado al GRP desde las LC. Desafortunadamente, este enfoque tiene limitaciones. El límite de velocidad para el tráfico de prioridad normal destinado al GRP es insuficiente para garantizar la protección a los datos del protocolo de ruteo de alta prioridad si un ataque se entrega a través de varias LC. La reducción del umbral en el que se descartan los datos de prioridad normal para proporcionar dicha protección sólo exacerba la pérdida de tráfico de administración de una inundación de prioridad normal.

Como muestra esta imagen, la rACL se ejecuta en cada LC antes de que el paquete se transmita al GRP.




Se requiere un mecanismo de protección para el GRP. Las rACL afectan el tráfico que se envía al GRP debido a las adyacencias de recepción. Las adyacencias de recepción son adyacencias de Cisco Express Forwarding para el tráfico destinado a las direcciones IP del router, como la dirección de broadcast o las direcciones configuradas en las interfaces del router. [3] Consulte la sección del apéndice para obtener más detalles sobre las adyacencias de recepción y los paquetes punteados.

El tráfico que ingresa a una LC se envía primero a la CPU local de la LC, y los paquetes que requieren procesamiento por el GRP se ponen en cola para reenviarlos al procesador de ruta. El ACL de recepción se crea en GRP y luego se envía hacia las CPU de las diferentes LC. Antes de que el tráfico se envíe desde la CPU LC al GRP, el tráfico se compara con la rACL. Si se permite, el tráfico pasa al GRP, mientras que el resto del tráfico se niega. Se inspecciona la rACL antes de la función LC a GRP que limita la velocidad. Debido a que rACL se usa para todas las adyacencias recibidas, algunos paquetes que son manejados por la CPU LC (tales como las solicitudes de eco) están sujetos también a filtrado rACL. Es necesario tener esto en cuenta cuando se diseñan entradas rACL.

Las ACL de recepción son parte uno de un rango de mecanismos de programa multiparte para proteger los recursos en un router. El trabajo futuro incluirá un componente de limitación de velocidad para la rACL.

## Impacto en el rendimiento

No se consume más memoria que la necesaria para mantener la entrada de configuración única y la propia lista de acceso definida. La rACL se copia a cada LC, por lo que se toma un área de memoria ligera en cada LC. En general, los recursos utilizados son minúsculos, especialmente si se comparan con los beneficios de la implementación.

Una ACL de recepción no afecta el rendimiento del tráfico reenviado. La rACL sólo se aplica para recibir tráfico de adyacencia. El tráfico reenviado nunca está sujeto a la rACL. El tráfico de tránsito se filtra con ACL de interfaz. Estas ACL "regulares" se aplican a las interfaces en una dirección

especificada. El tráfico está sujeto al procesamiento de ACL antes del procesamiento de rACL, por lo que el rACL no recibirá el tráfico denegado por la ACL de interfaz. [4]

La LC que realiza el filtrado real (es decir, la LC que recibe el tráfico filtrado por la rACL) tendrá mayor utilización de la CPU debido al procesamiento de la rACL. Sin embargo, esta mayor utilización de la CPU se debe a un gran volumen de tráfico destinado al GRP; el beneficio del GRP de la protección rACL es mucho mayor que el aumento de la utilización de la CPU en una LC. El uso de la CPU en una LC varía de acuerdo al tipo de motor de LC. Por ejemplo, dado el mismo ataque, una LC del motor 3 tendrá menor utilización de CPU que una LC 0 del motor.

La habilitación de turbo ACL (mediante el comando **access-list compilado**) convierte las ACL en una serie de entradas de tabla de búsqueda altamente eficiente. Cuando se habilitan las turbo ACL, la profundidad de rACL no afecta al rendimiento. En otras palabras, la velocidad de procesamiento es independiente del número de entradas en la ACL. Si la rACL es corta, las ACL turbo no aumentarán significativamente el rendimiento, sino que consumirán memoria; con las rACL cortas, las ACL compiladas probablemente no sean necesarias.

Al proteger el GRP, el rACL ayuda a garantizar la estabilidad del router y, en última instancia, de la red durante un ataque. Como se describe anteriormente, la rACL se procesa en la CPU de la LC, por lo que el uso de la CPU en cada LC aumentará cuando se dirija un gran volumen de datos al router. En los paquetes E0/E1 y algunos E2, el uso de la CPU del 100% puede conducir a caídas de protocolo de ruteo y capa de link. Estas pérdidas están localizadas en la tarjeta y los procesos de ruteo de GRP están protegidos, con lo que se mantiene la estabilidad. Las tarjetas E2 con microcódigo habilitado para regulación [5] activan el modo de regulación cuando se está bajo carga pesada y sólo reenvían tráfico de precedencia 6 y 7 al protocolo de ruteo. Otros tipos de motor tienen arquitecturas de cola múltiple; por ejemplo, las tarjetas E3 tienen tres colas para la CPU, con paquetes de protocolo de ruteo (precedencia 6/7) en una cola separada de alta prioridad. La CPU de LC alta, a menos que los paquetes de precedencia alta lo provoquen, no dará lugar a caídas del protocolo de ruteo. Los paquetes a las colas de menor prioridad se eliminarán de cola. Por último, las tarjetas basadas en E4 tienen ocho colas a la CPU, con una dedicada a los paquetes de protocolo de ruteo.

## Sintaxis

Se aplica una ACL de recepción con el siguiente comando de configuración global para distribuir la rACL a cada LC en el router.

```
[no] ip receive access-list
```

En esta sintaxis, *<num>* se define de la siguiente manera.

```
<1-199> IP access list (standard or extended)
<1300-2699> IP expanded access list (standard or extended)
```

## Ejemplos básicos de plantillas y ACL

Para poder utilizar este comando, debe definir una lista de acceso que identifique el tráfico que debería poder comunicarse con el router. La lista de acceso debe incluir ambos protocolos de ruteo así como la administración de tráfico (Protocolo de gateway de frontera [BGP], Abrir la ruta

más corta primero [OSPF], SNMP, SSH, Telnet). Para obtener más detalles, consulte la sección de pautas de despliegue.

La siguiente ACL de ejemplo proporciona un esquema simple y presenta algunos ejemplos de configuración que pueden adaptarse para usos específicos. El ACL ilustra las configuraciones necesarias para varios protocolos/servicios que se necesitan normalmente. Para SSH, Telnet y SNMP, se utiliza una dirección de loopback como destino. Para los protocolos de ruteo, se utiliza la dirección de interfaz real. La elección de interfaces de router que se utilizará en la rACL está determinada por políticas y operaciones del sitio local. Por ejemplo, si se utilizan loopbacks para todas las sesiones de peering BGP, sólo se deben permitir esos loopbacks en las sentencias **permit** para BGP.

```
!--- Permit BGP. access-list 110 permit tcp host bgp_peer host loopback eq bgp !--- Permit OSPF.
access-list 110 permit ospf host ospf_neighbor host 224.0.0.5 !--- Permit designated router
multicast address, if needed. access-list 110 permit ospf host ospf_neighbor host 224.0.0.6
access-list 110 permit ospf host ospf_neighbor host local_ip !--- Permit Enhanced Interior
Gateway Routing Protocol (EIGRP). access-list 110 permit eigrp host eigrp_neighbor host
224.0.0.10 access-list 110 permit eigrp host eigrp_neighbor host local_ip !--- Permit remote
access by Telnet and SSH. access-list 110 permit tcp management_addresses host loopback eq 22
access-list 110 permit tcp management_addresses host loopback eq telnet !--- Permit SNMP.
access-list 110 permit udp host NMS_stations host loopback eq snmp !--- Permit Network Time
Protocol (NTP). access-list 110 permit udp host ntp_server host loopback eq ntp !--- Router-
originated traceroute: !--- Each hop returns a message that time to live (ttl) !--- has been
exceeded (type 11, code 3); !--- the final destination returns a message that !--- the ICMP port
is unreachable (type 3, code 0). access-list 110 permit icmp any any ttl-exceeded access-list
110 permit icmp any any port-unreachable !--- Permit TACACS for router authentication. access-
list 110 permit tcp host tacacs_server router_src established !--- Permit RADIUS. access-list
110 permit udp host radius_server router_src log !--- Permit FTP for IOS upgrades. access-list
110 permit tcp host image_server eq ftp host router_ip_address access-list 110 permit tcp host
image_sever eq ftp-data host router_ip_address
```

Al igual que con todas las ACL de Cisco, hay una sentencia **deny** implícita al final de la lista de acceso, por lo que cualquier tráfico que no coincida con una entrada en la ACL será denegado.

**Nota:** La palabra clave **log** se puede utilizar para ayudar a clasificar el tráfico destinado al GRP que no está permitido. Aunque la palabra clave **log** proporciona información valiosa sobre los detalles de los resultados de ACL, los golpes excesivos a una entrada de ACL que utiliza esta palabra clave aumentarán el uso de CPU de LC. El impacto del rendimiento asociado con el registro variará con el tipo de motor LC. En general, el registro sólo debe utilizarse cuando sea necesario en los motores 0/1/2. Para los motores 3/4/4+, el registro tiene un impacto mucho menor debido al aumento del rendimiento de la CPU y a la arquitectura de cola múltiple.

El nivel de granularidad de esta lista de acceso está determinado por la política de seguridad local (por ejemplo, el nivel de filtrado requerido para vecinos OSPF).

## rACLS paquetes fragmentados

Las ACL tienen una palabra clave **fragments** que habilita un comportamiento especializado de manejo de paquetes fragmentado. En general, los fragmentos no iniciales que coinciden con las sentencias L3 (independientemente de la información L4) en una ACL se ven afectados por la sentencia **permit** o **deny** de la entrada coincidente. Tenga en cuenta que el uso de la palabra clave **fragments** puede obligar a las ACL a denegar o permitir fragmentos no iniciales con más granularidad.

En el contexto rACL, el filtrado de fragmentos agrega una capa adicional de protección contra un ataque DoS que utiliza sólo fragmentos no iniciales (como FO > 0). Al utilizar una sentencia deny para fragmentos no iniciales al comienzo de la rACL, se deniega el acceso al router a todos los fragmentos no iniciales. En raras circunstancias, una sesión válida podría requerir fragmentación y, por lo tanto, se filtraría si existe una instrucción **deny fragment** en la rACL.

Por ejemplo, considere la ACL parcial que se muestra a continuación.

```
access-list 110 deny tcp any any fragments
access-list 110 deny udp any any fragments
access-list 110 deny icmp any any fragments
<rest of ACL>
```

Al agregar estas entradas al principio de una rACL se deniega cualquier acceso de fragmento no inicial al GRP, mientras que los paquetes no fragmentados o los fragmentos iniciales pasan a las siguientes líneas de la rACL que no se ven afectadas por las instrucciones **deny fragment**. El fragmento rACL anterior también facilita la clasificación del ataque, ya que cada protocolo (protocolo de datagrama universal (UDP), TCP e ICMP) aumenta los contadores separados en la ACL.

Refiérase a Listas de Control de Acceso y Fragmentos de IP para obtener una explicación detallada de las opciones.

# Evaluación de riesgo

Asegúrese de que la rACL no filtra el tráfico crítico como los protocolos de ruteo o el acceso interactivo a los routers. El filtrado del tráfico necesario podría dar como resultado la incapacidad de acceder de forma remota al router, lo que requeriría una conexión de consola. Por esta razón, las configuraciones de laboratorio deben imitar la implementación real lo más cerca posible.

Como siempre, Cisco recomienda probar esta función en el laboratorio antes de la implementación.

# Apéndices y notas

## Recibir adyacencias y paquetes liberados

Como se describió anteriormente en este documento, algunos paquetes requieren procesamiento GRP. Los paquetes son impulsados desde el plano de reenvío de datos hacia el GRP. Esta es una lista de las formas comunes de datos de Capa 3 que requieren acceso GRP.

- Protocolos de ruteo
- Tráfico de control de multidifusión (OSPF, protocolo de router en espera en caliente [HSRP], protocolo de distribución de etiquetas [TDP], multidifusión independiente de protocolo [PIM], etc.)
- Paquetes MPLS (Multiprotocol Label Switching) que necesitan fragmentación
- Paquetes con ciertas opciones IP, como por ejemplo alerta del router.
- Primer paquete de flujos de multidifusión
- Paquetes ICMP fragmentados que requieren reensamblado

- Todo el tráfico destinado al router mismo (excepto el tráfico manejado en la LC)

Dado que las rACL se aplican a las adyacencias de recepción, la rACL filtra parte del tráfico que no se envía al GRP sino que es una adyacencia de recepción. El ejemplo más común de esto es una petición de eco ICMP (ping). Las solicitudes de eco ICMP dirigidas al router son manejadas por la CPU LC; dado que las solicitudes son adyacencias de recepción, también son filtradas por la rACL. Por lo tanto, para permitir pings en las interfaces (o en los loops de retorno) del router, el rACL debe permitir expresamente las solicitudes de eco.

Las adyacencias de recepción se pueden visualizar mediante el comando show ip cef.

```
12000-1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
1.1.1.1/32          attached            Null0
2.2.2.2/32          receive
64.0.0.0/30         attached            ATM4/3.300
...
```

## Pautas de implementación

Cisco recomienda prácticas de implementación conservadoras. Para implementar rACL correctamente, los requisitos de acceso del plano de control y gestión existentes deben entenderse bien. En algunas redes, puede ser difícil determinar el perfil de tráfico exacto necesario para crear las listas de filtrado. Las siguientes pautas describen un enfoque muy conservador para desplegar los rACL, utilizando las configuraciones interactivas rACL para identificar y eventualmente filtrar el tráfico.

1. **Identifique los protocolos utilizados en la red con una ACL de clasificación.**Implemente una rACL que permita todos los protocolos conocidos que acceden al GRP. Esta rACL de "detección" debe tener las direcciones de origen y de destino configuradas en **any**. El registro se puede utilizar para desarrollar una lista de direcciones de origen que coincidan con las instrucciones **permit** de protocolo. Además de la sentencia **permit** de protocolo, un **permit any log** line al final de la rACL se puede utilizar para identificar otros protocolos que serían filtrados por la rACL y que podrían requerir acceso al GRP.El objetivo es determinar qué protocolos utiliza la red específica. El registro se debe utilizar para el análisis para determinar "qué más" podría estar comunicándose con el router.**Nota:** Aunque la palabra clave **log** proporciona información valiosa sobre los detalles de los resultados de ACL, los golpes excesivos a una entrada de ACL que utiliza esta palabra clave pueden dar como resultado un número abrumador de entradas de registro y posiblemente un uso elevado de la CPU del router. Use la palabra clave del registro para períodos de tiempo cortos y sólo cuando sea necesaria para ayudar a clasificar el tráfico.
2. **Revise los paquetes identificados y comience a filtrar el acceso al GRP.**Una vez identificados y controlados los paquetes filtrados por el rACL en el paso 1, implemente un rACL con un permit any statement para los protocolos permitidos. Al igual que en el paso 1, la palabra clave **log** puede proporcionar más información sobre los paquetes que coinciden con las entradas **permit**. El uso de deny any en el final puede ayudar a identificar cualquier paquete inesperado destinado a GRP. Esta rACL proporcionará protección básica y les permitirá a los ingenieros de red garantizar que esté permitido todo el tráfico necesario.El objetivo es probar el rango de protocolos que necesitan comunicarse con el router sin tener el rango explícito de direcciones IP de origen y destino.
3. **Restrinja un rango de macros de direcciones de origen.**Sólo permita el rango total de su

bloque de ruteo interdominio sin clase (CIDR) asignado como dirección de origen. Por ejemplo, si se le ha asignado 171.68.0.0/16 para su red, permita las direcciones de origen desde sólo 171.68.0.0/16.Este paso minimiza el riesgo sin interrumpir ningún servicio. También proporciona puntos de datos de dispositivos/personas de fuera de su bloque CIDR que podrían estar accediendo a su equipo. Se descartará toda la dirección externa.Los peers BGP externos requerirán una excepción, ya que las direcciones de origen permitidas para la sesión estarán fuera del bloque CIDR.Esta fase puede dejarse por unos días para que recolecte datos para la siguiente fase de restricción de rACL.

4. **Reduzca las sentencias permit rACL para permitir solamente las direcciones de origen autorizadas conocidas.**Limite cada vez más la dirección de origen para permitir solamente los orígenes que se comunican con el GRP.
5. **Limite las direcciones de destino en la rACL. (opcional)**Algunos proveedores de servicios de Internet (ISP) pueden optar por permitir que únicamente ciertos protocolos específicos utilicen direcciones de destino específicas en el router. Esta fase final tiene el objeto de limitar el rango de direcciones de destino que admitirán tráfico para un protocolo. [6]

## Ejemplo de implementación

El siguiente ejemplo muestra una ACL de recepción que protege un router teniendo en cuenta el siguiente direccionamiento.

- El bloque de dirección de ISP es 169.223.0.0/16.
- El bloque de infraestructura del ISP es 169.223.252.0/22.
- El loopback para el router es 169.223.253.1/32.
- El router es un router de estructura básica de núcleo, por lo cual sólo las sesiones BGP internas se encuentran activas.

Dada esta información, la ACL inicial de recepción podría ser algo así como el siguiente ejemplo. Ya que se conoce el bloque de dirección de infraestructura, en un principio se permitirá el bloque completo. Más adelante, se añadirán entradas de control de acceso (ACE) más detalladas a medida que se obtengan las direcciones específicas para todos los dispositivos que necesitan acceso al router.

```
!
no access-list 110
!
!--- This ACL is an explicit permit ACL. !--- The only traffic permitted will be packets that !-
-- match an explicit permit ACE.

!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Explicit Permit !--- Permit only applications whose destination address !--- is
the loopback and whose source addresses !--- come from an valid host.

!
!--- Note: This template must be tuned to the network's !--- specific source address
environment. Variables in !--- the template need to be changed.

!
!--- Permit BGP. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq bgp
! !--- Permit OSPF. ! access-list 110 permit ospf 169.223.252.0 0.0.3.255 host 224.0.0.5 ! !---
Permit designated router multicast address, if needed. ! access-list 110 permit ospf
169.223.252.0 0.0.3.255 host 224.0.0.6 access-list 110 permit ospf 169.223.252.0 0.0.3.255 host
169.223.253.1 ! !--- Permit EIGRP. ! access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host
```

```
224.0.0.10 access-list 110 permit eigrp 169.223.252.0 0.0.3.255 host 169.223.253.1 ! !--- Permit
remote access by Telnet and SSH. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq 22 access-list 110 permit tcp 169.223.252.0 0.0.3.255 host 169.223.253.1 eq
telnet ! !--- Permit SNMP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255 host
169.223.253.1 eq snmp ! !--- Permit NTP. ! access-list 110 permit udp 169.223.252.0 0.0.3.255
host 169.223.253.1 eq ntp ! !--- Router-originated traceroute: !--- Each hop returns a message
that ttl !--- has been exceeded (type 11, code 3); !--- the final destination returns a message
that !--- the ICMP port is unreachable (type 3, code 0). ! access-list 110 permit icmp any
169.223.253.1 ttl-exceeded access-list 110 permit icmp any 169.223.253.1 port-unreachable ! !---
Permit TACACS for router authentication. ! access-list 110 permit tcp 169.223.252.0 0.0.3.255
host 169.223.253.1 established ! !--- Permit RADIUS. ! ! access-list 110 permit udp
169.223.252.0 0.0.3.255 169.223.253.1 log ! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !---
Phase 2 - Explicit Deny and Reaction !--- Add ACEs to stop and track specific packet types !---
that are destined for the router. This is the phase !--- where you use ACEs with counters to
track and classify attacks.

!
!--- SQL WORM Example - Watch the rate of this worm. !--- Deny traffic destined to UDP ports
1434 and 1433. !--- from being sent to the GRP. This is the SQL worm. ! access-list 110 deny udp
any any eq 1433 access-list 110 deny udp any any eq 1434 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Denies for
Tracking !--- Deny all other traffic, but count it for tracking.

!
access-list 110 deny udp any any
access-list 110 deny tcp any any range 0 65535
access-list 110 deny ip any any
```

## Notas

1. Consulte Introducción al Descarte selectivo de paquetes (SPD) y pautas de cola de retención para el aumento de la resistencia contra DoS.
2. Para obtener más información sobre Cisco Express Forwarding y adyacencias, refiérase a Descripción General de Cisco Express Forwarding.
3. Para obtener una descripción detallada de las pautas de implementación de ACL y los comandos relacionados, refiérase a Implementación de ACL en Cisco 12000 Series Internet Routers.
4. Esto se refiere a los agrupamientos Vanilla, a la Contabilidad de políticas del Protocolo de gateway de borde (BGPPA), al Control de velocidad por cada interfaz (PIRC) y a los paquetes de Regulación del tráfico de Frame Relay (FRTP).
5. La fase II de la protección de la ruta de recepción permitirá la creación de una interfaz de administración, limitando automáticamente qué dirección IP escuchará los paquetes entrantes.

# Información Relacionada

- Páginas de Soporte de Listas de Acceso
- Soporte Técnico - Cisco Systems