Protección del núcleo: Listas de control de acceso para la protección de la infraestructura

Contenido

Introducción

Este documento presenta pautas y técnicas de despliegue recomendadas para listas de control de acceso (ACL) de protección de infraestructura. Las ACL de infraestructuras sirven para reducir al mínimo el riesgo y la eficacia de ataques directos a la infraestructura permitiendo explícitamente solo el tráfico autorizado al equipo de infraestructura, a la vez que permitiendo el resto del tráfico de tránsito.

Protección de la infraestructura

Background

En un esfuerzo por proteger los routers de diversos riesgos (tanto accidentales como malintencionados), las ACL de protección de infraestructura deben implementarse en los puntos de ingreso de la red. Estas ACL IPv4 e IPv6 deniegan el acceso desde fuentes externas a todas las direcciones de infraestructura, como las interfaces del router. Al mismo tiempo, las ACL permiten que el tráfico de tránsito rutinario fluya sin interrupciones y proporcionan RFC 1918 básico, RFC 3330 y filtrado anti-simulación.

Los datos recibidos por un router pueden dividirse en dos categorías generales:

- tráfico que pasa a través del router a través de la ruta de reenvío
- tráfico destinado al router a través de la ruta de recepción para el manejo del procesador de

routing

En las operaciones normales, la gran mayoría del tráfico simplemente fluye a través de un router en ruta hacia su destino final.

Sin embargo, el procesador de routing (RP) debe gestionar determinados tipos de datos directamente, principalmente protocolos de routing, acceso de router remoto (como Secure Shell [SSH]) y tráfico de administración de red, como el protocolo simple de administración de red (SNMP). Además, los protocolos como el protocolo de mensajes de control de Internet (ICMP) y las opciones de IP pueden requerir el procesamiento directo por parte del RP. La mayoría de las veces, el acceso directo al router de la infraestructura sólo se requiere de fuentes internas. Algunas excepciones notables incluyen el peering BGP (Border Gateway Protocol) externo, protocolos que terminan en el router real (como el encapsulamiento de ruteo genérico [GRE] o IPv6 sobre túneles IPv4), y paquetes ICMP potencialmente limitados para pruebas de conectividad como solicitud de eco o mensajes ICMP inalcanzables y mensajes caducados de tiempo de vida (TTL) para traceroute.

Nota: Recuerde que el ICMP se utiliza a menudo para ataques simples de denegación de servicio (DoS) y sólo se debe permitir desde fuentes externas si es necesario.

Todos los RP tienen un sobre de rendimiento en el que funcionan. El tráfico excesivo destinado al RP puede saturar al router. Esto causa un uso elevado de la CPU y, en última instancia, da lugar a caídas del paquete y del protocolo de ruteo que provocan una denegación de servicio. Al filtrar el acceso a los routers de infraestructura desde fuentes externas, se mitigan muchos de los riesgos externos asociados con un ataque directo al router. Los ataques de origen externo ya no pueden acceder al equipo de infraestructura. El ataque se descarta en las interfaces de ingreso en el sistema autónomo (AS).

Las técnicas de filtro descritas en este documento tienen por objetivo filtrar los datos destinados al equipo de infraestructura de la red. No confunda el filtrado de la infraestructura con el filtrado genérico. El único propósito de la ACL de protección de infraestructura es restringir en un nivel granular qué protocolos y orígenes pueden acceder a equipos de infraestructura críticos.

Los equipos de infraestructura de red abarcan estas áreas:

- Todas las direcciones de administración de routers y switches, incluidas las interfaces de loopback
- Todas las direcciones de link internas: links de router a router (acceso de punto a punto y múltiple)
- Servidores o servicios internos a los que no se debe acceder desde fuentes externas

En este documento, todo el tráfico no destinado a la infraestructura se denomina a menudo tráfico de tránsito.

Técnicas

La protección de la infraestructura se puede lograr mediante una variedad de técnicas:

- **ACL de recepción (rACL)**Las plataformas Cisco 12000 y 7500 admiten rACL que filtran todo el tráfico destinado al RP y no afectan al tráfico de tránsito. El tráfico autorizado se debe permitir explícitamente y la rACL se debe implementar en cada router. Consulte GSR: Recibir listas de control de acceso para obtener más información.
- **ACL de router salto por salto**Los routers también se pueden proteger mediante la definición

de ACL que permiten solamente el tráfico autorizado a las interfaces del router, denegando todos los demás excepto el tráfico de tránsito, que se debe permitir explícitamente. Esta ACL es lógicamente similar a una rACL pero afecta al tráfico de tránsito y, por lo tanto, puede tener un impacto negativo en el rendimiento de la velocidad de reenvío de un router.

- **Filtrado perimetral mediante ACL de infraestructura**Las ACL se pueden aplicar al borde de la red. En el caso de un proveedor de servicios (SP), éste es el borde del AS. Esta ACL filtra explícitamente el tráfico destinado al espacio de direcciones de infraestructura. La implementación de las ACL de infraestructura perimetral requiere que defina claramente su espacio de infraestructura y los protocolos requeridos/autorizados que acceden a este espacio. La ACL se aplica al ingreso a la red en todas las conexiones con cara externa, como conexiones de iguales, conexiones de clientes, etc.Este documento se centra en el desarrollo y despliegue de ACL de protección de infraestructura de borde.

Ejemplos de ACL

Estas listas de acceso IPv4 e IPv6 proporcionan ejemplos simples pero realistas de entradas típicas requeridas en una ACL de protección. Estas ACL básicas deben personalizarse con los detalles de configuración específicos del sitio local. En entornos IPv4 e IPv6 duales, se implementan ambas listas de acceso.

Ejemplo de IPv4

```
!--- Anti-spoofing entries are shown here. !--- Deny special-use address sources. !--- Refer to RFC 3330 for additional special use addresses. access-list 110 deny ip host 0.0.0.0 any access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255 any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list 110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. access-list 110 deny ip YOUR_CIDR_BLOCK any !--- Permit BGP. access-list 110 permit tcp host bgp_peer host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host router_ip !--- Deny access to internal infrastructure addresses. access-list 110 deny ip any INTERNAL_INFRASTRUCTURE_ADDRESSES !--- Permit transit traffic. access-list 110 permit ip any any
```

Ejemplo de IPv6

La lista de acceso IPv6 debe aplicarse como una lista de acceso extendida y denominada.

```
!--- Configure the access-list. ipv6 access-list iacl !--- Deny your space as source from entering your AS. !--- Deploy only at the AS edge. deny ipv6 YOUR_CIDR_BLOCK_IPV6 any !--- Permit multiprotocol BGP. permit tcp host bgp_peer_ipv6 host router_ipv6 eq bgp permit tcp host bgp_peer_ipv6 eq bgp host router_ipv6 !--- Deny access to internal infrastructure addresses. deny ipv6 any INTERNAL_INFRASTRUCTURE_ADDRESSES_IPV6 !--- Permit transit traffic. permit ipv6 any any
```

Nota: La palabra clave **log** se puede utilizar para proporcionar detalles adicionales sobre el origen y los destinos de un protocolo determinado. Aunque esta palabra clave proporciona información valiosa sobre los detalles de los resultados de ACL, los golpes excesivos a una entrada de ACL que utiliza la palabra clave **log** aumentan la utilización de la CPU. El impacto del rendimiento asociado con el registro varía de acuerdo a la plataforma. Además, el uso de la palabra clave log inhabilita el switching de Cisco Express Forwarding (CEF) para los paquetes que coinciden con la sentencia de lista de acceso. Dichos paquetes, por el contrario, son switcheados rápidamente.

Desarrollar una ACL de protección

En general, una ACL de infraestructura se compone de cuatro secciones:

- Dirección de uso especial y entradas protegidas contra imitación que impiden que fuentes ilegítimas y paquetes con direcciones de origen que pertenecen a su AS ingresen al AS desde una fuente externa**Nota:** RFC 3330 define las direcciones de uso especial de IPv4 que pueden requerir filtrado. RFC 1918 define el espacio de dirección IPv4 reservado que no es una dirección válida en Internet. RFC 3513 define la arquitectura de direccionamiento de IP. RFC 2827 proporciona pautas de filtrado de ingreso.
- Tráfico con origen externo explícitamente permitido destinado a direcciones de infraestructura
- **los enunciados de negación correspondientes a todo el tráfico generado externamente para brindar infraestructura a las direcciones**
- sentencias **permit** para el resto del tráfico para el tráfico de estructura básica normal en ruta a destinos que no son de infraestructura

La línea final en la ACL de infraestructura permite explícitamente el tráfico de tránsito: **permit ip any any para IPv4 y permit ipv6 any any para IPv6.** Esta entrada asegura que todos los protocolos IP tengan permiso a través del núcelo y que los clientes puedan continuar ejecutando aplicaciones sin problemas.

El primer paso cuando se desarrolla una ACL de protección de infraestructura es comprender los protocolos requeridos. Aunque cada sitio tiene requisitos específicos, ciertos protocolos se suelen implementar y deben entenderse. Por ejemplo, se debe permitir explícitamente el BGP externo a los peers externos. También se debe permitir explícitamente cualquier otro protocolo que requiera acceso directo al router de infraestructura. Por ejemplo, si finaliza un túnel GRE en un router de infraestructura de núcleo, también se debe permitir explícitamente el protocolo 47 (GRE). Del mismo modo, si finaliza un túnel IPv6 sobre IPv4 en un router de infraestructura de núcleo, también se debe permitir explícitamente el protocolo 41 (IPv6 sobre IPv4).

Se puede utilizar una ACL de clasificación para ayudar a identificar los protocolos requeridos. La ACL de clasificación se compone de instrucciones **permit** para los diversos protocolos que se pueden destinar a un router de infraestructura. Refiérase al apéndice sobre los protocolos IP soportados en Cisco IOS® Software para obtener una lista completa. El uso del comando **show access-list** para mostrar un conteo de aciertos de entrada de control de acceso (ACE) identifica los protocolos requeridos. Los resultados sospechosos o sorprendentes deben investigarse y entenderse antes de crear declaraciones de **permiso** para protocolos inesperados.

Por ejemplo, esta ACL IPv4 ayuda a determinar si se debe permitir la tunelización GRE, IPsec (ESP) e IPv6 (protocolo IP 41).

```
access-list 101 permit GRE any infrastructure_ips
access-list 101 permit ESP any infrastructure_ips
access-list 101 permit 41 any infrastructure_ips
access-list 101 permit ip any infrastructure_ips log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted.

access-list 101 permit ip any any

interface <int>
 ip access-group 101 in
```

Esta ACL IPv6 se puede utilizar para determinar si se debe permitir GRE e IPsec (ESP).

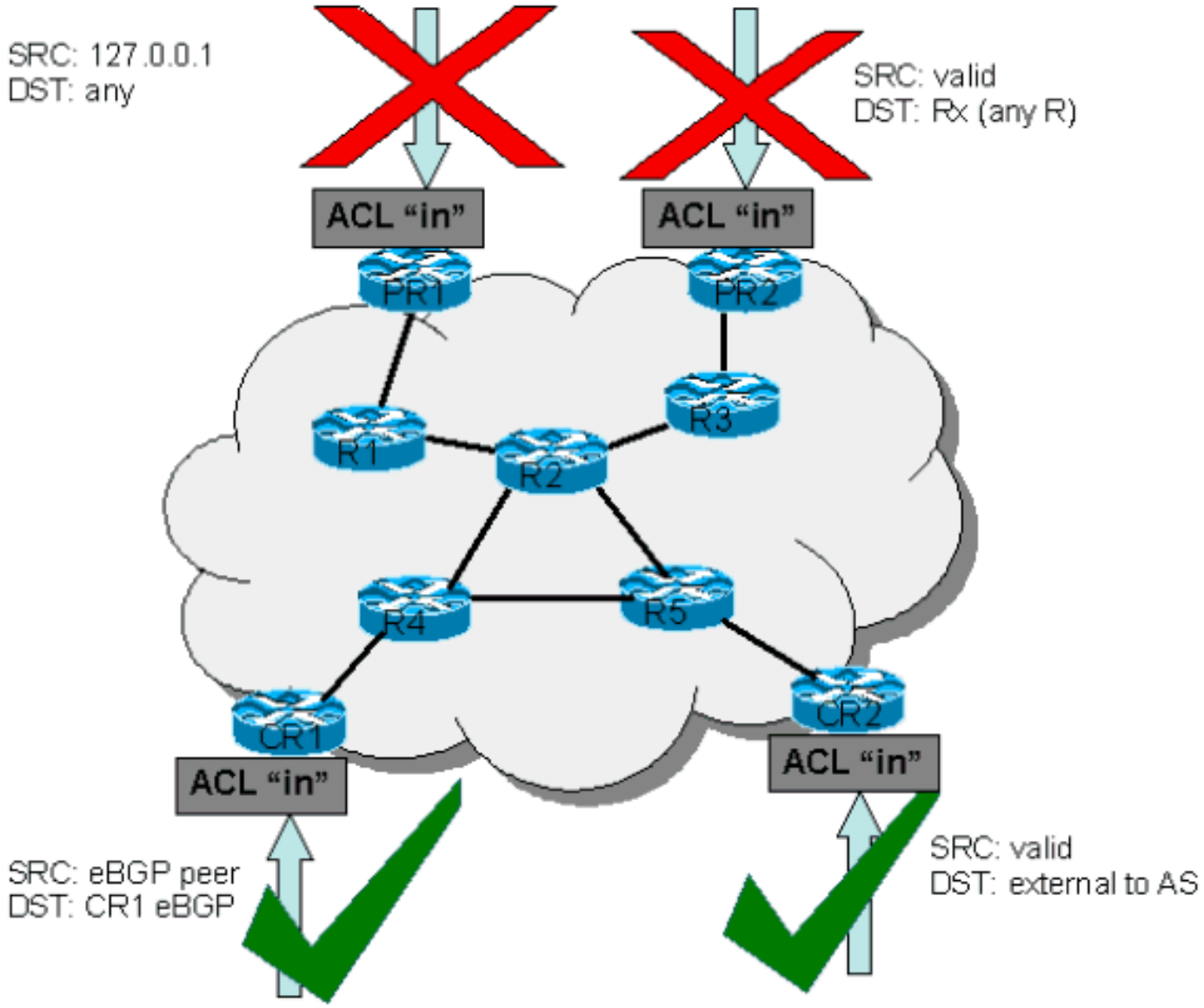
```
ipv6 access-list determine_protocols
 permit GRE any infrastructure_ips_ipv6
 permit ESP any infrastructure_ips_ipv6
 permit ipv6 any infrastructure_ips_ipv6 log
!--- The log keyword provides more details !--- about other protocols that are not explicitly
permitted. permit ipv6 any any interface <int> ipv6 traffic-filter determine_protocols in
```

Además de los protocolos requeridos, es necesario identificar el espacio de la dirección de la infraestructura, ya que éste es el espacio que protege la ACL. El espacio de direcciones de infraestructura incluye cualquier dirección que se utilice para la red interna y a la que rara vez acceden fuentes externas como interfaces de router, direccionamiento de link punto a punto y servicios de infraestructura críticos. Dado que estas direcciones se utilizan para la parte de destino de la infraestructura ACL, el resumen es crítico. Siempre que sea posible, estas direcciones se deben agrupar en bloques de routing entre dominios sin clase (CIDR).

Con el uso de los protocolos y las direcciones identificadas, la infraestructura ACL se puede construir para permitir los protocolos y proteger las direcciones. Además de la protección directa, la ACL también proporciona una primera línea de defensa contra ciertos tipos de tráfico inválido en Internet.

- Se debe denegar el espacio RFC 1918.
- Los paquetes con una dirección de origen que caen dentro del espacio de dirección de uso especial, como se define en RFC 3330, deben ser denegados.
- Se deben aplicar filtros antisimulación. (Su espacio de dirección nunca debe ser la fuente de paquetes de fuera de su AS.)

Esta ACL recién construida se debe aplicar de forma entrante en todas las interfaces de ingreso. Vea las secciones sobre pautas de implementación y ejemplos de implementación para obtener más detalles.



ACL y paquetes fragmentados

Las ACL tienen una palabra clave **fragments** que habilita un comportamiento especializado de manejo de paquetes fragmentado. Sin esta palabra clave **fragments**, los fragmentos no iniciales que coinciden con las sentencias de Capa 3 (independientemente de la información de Capa 4) en una ACL se ven afectados por la sentencia permit o deny de la entrada coincidente. Sin embargo, al agregar la palabra clave **fragments**, puede obligar a las ACL a denegar o permitir fragmentos no iniciales con más granularidad. Este comportamiento es el mismo para las listas de acceso IPv4 e IPv6, con la excepción de que, aunque las ACL IPv4 permiten el uso de la palabra clave fragments dentro de las sentencias de Capa 3 y Capa 4, las ACL IPv6 sólo permiten el uso de la palabra clave fragments dentro de las sentencias de Capa 3.

El filtrado de fragmentos agrega una capa adicional de protección contra un ataque de denegación de servicio (DoS) que utiliza fragmentos no iniciales (es decir, FO > 0). Al utilizar una sentencia deny para fragmentos no iniciales al comienzo de la ACL, 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 ACL.

Por ejemplo, considere esta IPv4ACL parcial:

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

La adición de estas entradas al principio de una ACL niega cualquier acceso de fragmento no inicial a los routers de núcleo, mientras que los paquetes no fragmentados o los fragmentos iniciales pasan a las siguientes líneas de la ACL no afectadas por las sentencias **deny fragment**. El comando ACL anterior también facilita la clasificación del ataque, ya que cada protocolo (protocolo de datagramas universales (UDP), TCP e ICMP) incrementa los contadores separados en la ACL.

Este es un ejemplo comparable para IPv6:

```
ipv6 access-list iacl
   deny ipv6 any infrastructure_IP fragments
```

La adición de esta entrada al principio de una ACL IPv6 deniega cualquier acceso de fragmento no inicial a los routers de núcleo. Como se ha señalado anteriormente, las listas de acceso IPv6 sólo permiten el uso de la palabra clave fragments dentro de las instrucciones de Capa 3.

Dado que varios ataques se basan en routers del núcleo de inundación con paquetes fragmentados, el filtrado de fragmentos entrantes en la estructura del núcleo proporciona una medida adicional de protección y ayuda a garantizar que un ataque no inyecte fragmentos al simplemente hacer coincidir las reglas de capa 3 en la infraestructura ACL.

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

Evaluación de riesgo

Tenga en cuenta estas dos áreas de riesgo clave al implementar ACL de protección de infraestructura:

- Asegúrese de que estén en vigor las declaraciones **permit/deny** apropiadas. Para que la ACL sea efectiva, se deben permitir todos los protocolos requeridos y el espacio de dirección correcto debe estar protegido por las sentencias **deny**.
- El rendimiento de la ACL varía de una plataforma a otra. Revise las características de rendimiento de su hardware antes de implementar ACL.

Como siempre, se recomienda probar este diseño en el laboratorio antes de la implementación.

Apéndices

Protocolos IP soportados en el software del IOS de Cisco

Estos protocolos IP son soportados por Cisco IOS Software:

- 1 - ICMP
- 2 - IGMP
- 3 - GGP
- 4 - IP en encapsulación IP
- 6 - TCP
- 8 - EGP
- 9 - IGRP
- 17 - UDP
- 20 - HMP
- 27 - RDP
- 41 - IPv6 en tunelización IPv4
- 46 - RSVP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 53 - BORRAR
- 54 - NARP
- 55 - Movilidad IP
- 63: cualquier red local
- 77 - Sun ND
- 80 - IP ISO
- 88 - EIGRP
- 89 - OSPF
- 90 - RPC de Sprite
- 91 - LARP
- 94 - IP sobre IP compatible con KA9Q/NOS
- 103 - PIM
- 108 - Compresión IP
- 112 - VRRP
- 113 - PGM
- 115 - L2TP
- 120 - UTI
- 132 - SCTP

Pautas de implementación

Cisco recomienda prácticas de implementación conservadoras. Para implementar correctamente las ACL de infraestructura, los protocolos requeridos deben entenderse bien y el espacio de dirección debe identificarse y definirse claramente. Estas directrices describen un método muy conservador para implementar ACL de protección mediante un enfoque iterativo.

1. **Identifique los protocolos utilizados en la red con una ACL de clasificación.**Implemente una ACL que permita todos los protocolos conocidos que acceden a los dispositivos de infraestructura. Esta ACL de detección tiene una dirección de origen de **cualquier** y un destino que abarca el espacio IP de la infraestructura. El registro se puede utilizar para desarrollar una lista de direcciones de origen que coincidan con las instrucciones **permit** de protocolo. Se requiere una última línea que permita **ip any any** (IPv4) o **ipv6 any** (IPv6) para permitir el flujo de tráfico.El objetivo es determinar qué protocolos utiliza la red específica. El

registro se utiliza 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. Además, el uso de la palabra clave **log** inhabilita el switching de Cisco Express Forwarding (CEF) para los paquetes que coinciden con la sentencia de lista de acceso. Dichos paquetes, por el contrario, son switcheados rápidamente. Use la palabra clave del registro para períodos de tiempo cortos y sólo cuando sea necesaria para ayudar a clasificar el tráfico.

2. **Analice los paquetes identificados y comience a filtrar el acceso al procesador de rutas (RP).**Una vez que se hayan identificado y revisado los paquetes que filtró la ACL en el paso 1, despliegue la ACL con un permit any source (Permitir cualquier fuente) para brindar infraestructura a las direcciones 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 los routers. La última línea de esta ACL debe ser una instrucción **permit ip any any** (IPv4) o **permit ipv6 any** (IPv6) para permitir el flujo del tráfico de tránsito. Esta ACL proporciona protección básica y permite a los ingenieros de red garantizar que se permite todo el tráfico necesario.
3. **Restrinja las direcciones de origen.**Una vez que comprenda claramente los protocolos que deben permitirse, puede realizarse un filtrado adicional para habilitar sólo las fuentes autorizadas para dichos protocolos. Por ejemplo, puede permitir explícitamente vecinos BGP externos o direcciones de peer GRE específicas.Este paso acota el riesgo sin suspender ningún servicio y le permite aplicar un control granular a las fuentes que acceden a la infraestructura del equipo.
4. **Limite las direcciones de destino en la ACL. (opcional)**Algunos proveedores de servicios de Internet (ISP) pueden optar por permitir que protocolos específicos utilicen direcciones de destino específicas en el router. Esta fase final está diseñada para limitar el rango de direcciones de destino que pueden aceptar el tráfico para un protocolo.

Ejemplos de implementación

Ejemplo de IPv4

Este ejemplo de IPv4 muestra una ACL de infraestructura que protege un router según este direccionamiento:

- El bloque de direcciones ISP es 169.223.0.0/16.
- El bloque de infraestructura ISP es 169.223.252.0/22.
- El loopback para el router es 169.223.253.1/32.
- El router es un router de pares y establece conexión entre pares con 169.254.254.1 (a la dirección 169.223.252.1).

La ACL de protección de infraestructura mostrada se desarrolla en función de la información anterior. La ACL permite el peering BGP externo al peer externo, proporciona filtros anti-simulación y protege la infraestructura de todo el acceso externo.

```
!
no access-list 110
```

```
!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing Denies !--- These ACEs deny fragments, RFC 1918 space, !--- invalid
source addresses, and spoofs of !--- internal space (space as an external source).

!
!--- Deny fragments to the infrastructure block. access-list 110 deny tcp any 169.223.252.0
0.0.3.255 fragments access-list 110 deny udp any 169.223.252.0 0.0.3.255 fragments access-list
110 deny icmp any 169.223.252.0 0.0.3.255 fragments !--- Deny special-use address sources. !---
See RFC 3330 for additional special-use addresses. access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any access-list 110 deny ip 192.0.2.0 0.0.0.255
any access-list 110 deny ip 224.0.0.0 31.255.255.255 any !--- Filter RFC 1918 space. access-list
110 deny ip 10.0.0.0 0.255.255.255 any access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any !--- Deny our internal space as an external
source. !--- This is only deployed at the AS edge access-list 110 deny ip 169.223.0.0
0.0.255.255 any !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--
- Permit only applications/protocols whose destination !--- address is part of the
infrastructure IP block. !--- The source of the traffic should be known and authorized.

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

!--- Permit external BGP. access-list 110 permit tcp host 169.254.254.1 host 169.223.252.1 eq
bgp access-list 110 permit tcp host 169.254.254.1 eq bgp host 169.223.252.1 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 - Explicit Deny to
Protect Infrastructure

access-list 110 deny ip any 169.223.252.0 0.0.3.255
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 4 - Explicit Permit for Transit Traffic

access-list 110 permit ip any any
```

Ejemplo de IPv6

Este ejemplo de IPv6 muestra una ACL de infraestructura que protege un router según este direccionamiento:

- El bloque de prefijo total asignado al ISP es 2001:0DB8::/32.
- El bloque de prefijo IPv6 utilizado por el ISP para las direcciones de la infraestructura de red es 2001:0DB8:C18::/48.
- Hay un router de peering BGP con una dirección IPv6 de origen de 2001:0DB8:C18:2:1::1 que hace peers con la dirección IPv6 de destino de 2001:0DB8:C19:2:1::F.

La ACL de protección de infraestructura mostrada se desarrolla en función de la información anterior. La ACL permite el peering BGP multiprotocolo externo al peer externo, proporciona filtros anti-simulación y protege la infraestructura de todo el acceso externo.

```
no ipv6 access-list iacl
ipv6 access-list iacl
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!--- Phase 1 - Anti-spoofing and Fragmentation Denies !--- These ACEs deny fragments and spoofs
of !--- internal space as an external source. !--- Deny fragments to the infrastructure block.
deny ipv6 any 2001:0DB8:C18::/48 fragments !--- Deny our internal space as an external source.
!--- This is only deployed at the AS edge. deny ipv6 2001:0DB8::/32 any
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 2 - Explicit Permit !--- Permit only
applications/protocols whose destination !--- address is part of the infrastructure IP block. !-
-- The source of the traffic should be known and authorized. !--- Note: This template must be
```

```
tuned to the !--- specific source address environment of the network. Variables in !--- the
template need to be changed. !--- Permit multiprotocol BGP. permit tcp host 2001:0DB8:C19:2:1::F
host 2001:0DB8:C18:2:1::1 eq bgp permit tcp host 2001:0DB8:C19:2:1::F eq bgp host
2001:0DB8:C18:2:1::1 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 3 -
Explicit Deny to Protect Infrastructure deny ipv6 any 2001:0DB8:C18::/48
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !--- Phase 4 - Explicit Permit for
Transit Traffic permit ipv6 any any
```

Información Relacionada

- Páginas de Soporte de Listas de Acceso
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems