Protección del núcleo: Listas de control de acceso de la Protección de la Infraestructura

Contenido

Introducción
Protección de la Infraestructura
Antecedente
Técnicas
Ejemplos de ACL
Desarrolle una protección ACL
ACL y paquetes fragmentados
Evaluación de riesgo
Apéndices
Protocolos IP soportados en el software del IOS de Cisco
Pautas para la instrumentación
Ejemplos de despliegue
Información Relacionada

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

Antecedente

En un esfuerzo para proteger al Routers contra los diversos riesgos — accidental y malévolo — la Protección de la Infraestructura ACL se debe desplegar en los puntos de ingreso a la red. Este IPv4 y el IPv6 ACL niegan el acceso de las fuentes externas a todos los direccionamientos de la infraestructura, tales como interfaces del router. Al mismo tiempo, el tráfico de tránsito de la rutina de permiso del ACL a fluir ininterrumpido y para proporcionar el RFC 1918 básico , el RFC 3330 , y el filtro protegido contra imitación.

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

- trafique que los pasos a través del router vía el trayecto de reenvío
- tráfico destinado para el router vía la trayectoria de la recepción para la dirección del Route

Processor

En los funcionamientos normales, el amplia mayoría de tráfico atraviesa simplemente a un router en el camino a su destino final.

Sin embargo, el (RP) del Route Processor debe manejar los tipos determinados de datos directamente, especialmente los Routing Protocol, acceso del router remoto (tal como shell seguro [SSH]), y tráfico de administración de red tal como Simple Network Management Protocol (SNMP). Además, los protocolos tales como Internet Control Message Protocol (ICMP) y las opciones IP pueden requerir el procesamiento directo por el RP. Lo más a menudo posible, el acceso directo del router de infraestructura se requiere solamente de las fuentes internas. Algunas excepciones notables incluyen el (BGP) del Border Gateway Protocol externo que mira, los protocolos que terminan en el router real (tal como [GRE] o IPv6 del Generic Routing Encapsulation sobre los túneles del IPv4), y los paquetes icmp potencialmente limitados para la prueba de la Conectividad tal como pedido de eco o los ICMP fuera de alcance y el Time to Live (TTL) expiraron los mensajes para el traceroute.

Nota: Recuerde que el ICMP es de uso frecuente para los ataques simples del servicio negado (DOS) y se debe permitir solamente de las fuentes externas en caso necesario.

Todos los RP tienen un sobre de rendimiento en el cual actúen. El tráfico excesivo destinado para el RP puede abrumar al router. Esto causa CPU elevada el uso y da lugar en última instancia al paquete y a los descensos del Routing Protocol que causan una negación de servicio. Filtrando el acceso a los routeres de infraestructura de las fuentes externas, muchos de los riesgos externos asociados a un ataque directo del router se atenúan. Los ataques externamente originados pueden no más el equipo de la infraestructura de acceso. El ataque se cae en las interfaces de ingreso en el sistema.

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 infraestructura con el filtrado genérico. El propósito singular de la Protección de la Infraestructura ACL es restringir en un nivel granular qué protocolos y fuentes pueden acceder el equipo de infraestructura crítico.

El equipo de la infraestructura de red abarca estas áreas:

- Todos los direccionamientos del router y del administrador de switches, incluyendo el loopback interconectan
- Todas las direcciones del link internas: el router a router conecta (Punto a punto y el acceso múltiple)
- Servidores internos o servicios que no deben ser accedidos de las fuentes externas

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

Técnicas

La Protección de la Infraestructura se puede alcanzar con una variedad de técnicas:

- **Reciba ACL (el rACLs)**Cisco 12000 y 7500 rACLs del soporte de Plataformas que filtran todo el tráfico destinado al RP y no afectan al tráfico de tránsito. El tráfico autorizado debe ser permitido explícitamente y el rACL se debe desplegar en cada router. Consulte GSR: Reciba las listas de control de acceso para más información.
- **Router ACLS del salto por el salto**El Routers puede también ser protegido definiendo los ACL

que permiten solamente el tráfico autorizado a las interfaces del router, negando todos los demás a excepción del tráfico de tránsito, que debe ser permitido explícitamente. Este ACL es lógicamente similar a un rACL pero afecta al tráfico de tránsito, y por lo tanto puede tener un impacto del rendimiento negativo en la velocidad de reenvío de un router.
- **Filtrado de borde vía la infraestructura ACL**Los ACL se pueden aplicar al borde de la red. En el caso de un proveedor de servicio (SP), éste es el borde del COMO. Este ACL filtra explícitamente el tráfico destinado para el espacio de la dirección de la infraestructura. El despliegue de la infrastructura de bordes ACL requiere que usted defina claramente su espacio de la infraestructura y protocolos requeridos/autorizados que accedan este espacio. El ACL es aplicado en el ingreso a su red en todos los conexión enfrentado a hacia afuera, tales como conexiones del peering, las conexiones del cliente, y así sucesivamente.Este documento se centra en el desarrollo y despliegue de ACL de protección de infraestructura de borde.

Ejemplos de ACL

Las Listas de acceso TheseIPv4 y del IPv6 proporcionan simple con todo los ejemplos realistas de las entradas típicas requeridas en una protección ACL. Estos ACL básicos necesitan ser personalizados con los detalles de la configuración específicos del sitio locales. En los entornos duales del IPv4 y del IPv6, se despliegan ambas listas de acceso.

Ejemplo del 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 del IPv6

La lista de acceso del IPv6 se debe aplicar como extendido, lista de acceso 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 de registro puede utilizarse para proporcionar más detalles acerca del origen y los destinos de un determinado protocolo. Aunque esta palabra clave proporcione el conocimiento valioso en los detalles de los golpes ACL, los golpes excesivos a una entrada ACL que utilice la palabra clave del **registro** aumentan la utilización de la CPU. El impacto del rendimiento asociado con el registro varía de acuerdo a la plataforma. También, usando el registro la palabra clave inhabilita el Cisco Express Forwarding (CEF) que conmuta para los paquetes que hacen juego la sentencia de lista de acceso. Dichos paquetes, por el contrario, son

switcheados rápidamente.

Desarrolle una protección ACL

Una infraestructura ACL se compone generalmente 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 direcciones IPv4 de uso especial que pueden llegar a 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. El RFC 2827 proporciona las guías de consulta del filtrado de ingreso.
- Tráfico externamente originado explícitamente permitido destinado a los direccionamientos de la infraestructura
- los enunciados de negación correspondientes a todo el tráfico generado externamente para brindar infraestructura a las direcciones
- **permita las** declaraciones para el resto del tráfico para el tráfico de estructura básica normal en el camino a los destinos del noninfrastructure

La línea final en la infraestructura ACL 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 usted desarrolla una Protección de la Infraestructura ACL es entender los protocolos requeridos. Aunque cada sitio tenga requisitos específicos, ciertos protocolos se despliegan y deben comúnmente ser entendidos. Por ejemplo, el BGP externo a los peeres externos necesita ser permitido explícitamente. Cualquier otros protocolos que requieran el acceso directo a la necesidad del router de infraestructura de ser permitido explícitamente también. Por ejemplo, si usted termina un túnel GRE en un router de la infraestructura esencial, después del protocolo 47 del (GRE) necesidades también de ser permitido explícitamente. Semejantemente, si usted termina un IPv6 sobre el túnel del IPv4 en un router de la infraestructura esencial, después necesidades del protocolo 41 (IPv6 sobre el IPv4) también de ser permitido explícitamente.

Una clasificación ACL se puede utilizar para ayudar a identificar los protocolos requeridos. La clasificación ACL se compone de las declaraciones del **permiso** para los diversos protocolos que pueden ser destinados para un router de infraestructura. Refiera al apéndice en los protocolos soportados IP en el software de Cisco IOS® para una lista completa. El uso del comando del **comando show access-list** de visualizar una cuenta de los golpes de la Entrada de control de acceso (ACE) identifica los protocolos requeridos. Los resultados sospechosos o asombrosamente deben ser investigados y ser entendidos antes de que usted cree las declaraciones del **permiso** para los protocolos inesperados.

Por ejemplo, este las ayudas del IPv4 ACL determinan si GRE, el IPSec (ESP) y IPv6 que hace un túnel (protocolo IP la necesidad de 41) de ser permitido.

```
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
```

Este IPv6 ACL se puede utilizar para determinar si el GRE y el IPSec (ESP) necesitan ser permitidos.

```
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, el espacio de la dirección de la infraestructura necesita ser identificado puesto que éste es el espacio que el ACL protege. El espacio de la dirección de la infraestructura incluye cualquier direccionamiento que se utilice para la red interna y sea accedido raramente por las fuentes externas tales como interfaces del router, dirección de enlace punto a punto, y servicios críticos de la infraestructura. Puesto que estos direccionamientos se utilizan para la porción de destino de la infraestructura ACL, el resumen es crítico. Donde sea posible, estos direccionamientos se deben agrupar en los bloques del Classless Interdomain Routing (CIDR).

Con el uso de los protocolos y de los direccionamientos identificados, la infraestructura ACL se puede construir para permitir los protocolos y para proteger los direccionamientos. Además de la protección directa, el ACL también proporciona una primera línea de defensa contra los tipos determinados de tráfico no válido en Internet.

- El espacio del RFC 1918 debe ser negado.
- Los paquetes con una dirección de origen que caen bajo espacio de la dirección del especial-uso, según lo definido en el RFC 3330, deben ser negados.
- los filtros del Anti-spoof deben ser aplicados. (Su espacio de la dirección debe nunca ser la fuente de paquetes del exterior su COMO.)

Este ACL nuevamente construido debe ser entrante aplicado en todas las interfaces de ingreso. Vea las secciones en las Pautas para la instrumentación y los ejemplos de despliegue para más detalles.

ACL y paquetes fragmentados

Los ACL tienen una palabra clave de los **fragmentos** que habilite el comportamiento hecho fragmentos especializado de la dirección del paquete. Sin esta palabra clave de los **fragmentos**, los fragmentos noninitial que hacen juego las declaraciones de la capa 3 (con independencia de la información de la capa 4) en un ACL son afectados por la declaración del permit or deny de la entrada correspondida con. Sin embargo, agregando los **fragmentos** palabra clave, usted puede forzar los ACL a niega o permite los fragmentos noninitial con más granularity. Este comportamiento es lo mismo para las listas de acceso del IPv4 y del IPv6, con excepción del hecho que, mientras que el IPv4 ACL permite el uso de la palabra clave de los fragmentos dentro de las declaraciones de la capa 3 y de la capa 4, el IPv6 ACL permite solamente el uso de la palabra clave de los fragmentos dentro de las declaraciones de la capa 3.

La filtración de los fragmentos agrega una capa adicional de protección contra un ataque de Negación de servicio (DoS) que utilice los fragmentos noninitial (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. Bajo circunstancias poco probables, una sesión válida pudo requerir la fragmentación, y por lo tanto se filtre si una declaración del **fragmento de la negación** existe en el ACL.

Por ejemplo, considere este 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 un ACL niega cualquier acceso noninitial del fragmento a los routeres del núcleo, mientras que los paquetes no fragmentados o los fragmentos iniciales pasan a las líneas siguientes del ACL inafectado por las declaraciones del **fragmento de la negación**. El comando acl precedente también facilita la clasificación del ataque desde cada protocolo — el Datagram Protocol universal (UDP), TCP, y ICMP — los incrementos separa los contadores en el ACL.

Esto es un ejemplo comparable para el IPv6:

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

La adición de esta entrada al principio de un IPv6 ACL niega cualquier acceso noninitial del fragmento a los routeres del núcleo. Según lo observado previamente, las listas de acceso del IPv6 permiten solamente el uso de la palabra clave de los fragmentos dentro de las declaraciones de la 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.

Refiera a las listas de control de acceso y a los fragmentos IP para una explicación detallada de las opciones.

Evaluación de riesgo

Considere estas dos áreas del riesgo dominante cuando usted despliega la Protección de la Infraestructura ACL:

- Asegúrese de que el **permiso**/los **enunciados de negación** apropiados exista. Para que el ACL sea eficaz, todos los protocolos requeridos deben ser permitidos y el espacio de dirección correcta se debe proteger por los **enunciados de negación**.
- El rendimiento de las ACL varía de la plataforma a la plataforma. Revise las características del rendimiento de su hardware antes de que usted despliegue los ACL.

Como siempre, se recomienda que usted prueba este diseño en el laboratorio antes del despliegue.

Apéndices

Protocolos IP soportados en el software del IOS de Cisco

Estos protocolos IP son soportados por el Cisco IOS Software:

- 1 – ICMP

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

Pautas para la instrumentación

Cisco recomienda las prácticas conservadoras del despliegue. Para desplegar con éxito la infraestructura ACL, los protocolos requeridos deben ser entendidos bien, y el espacio de la dirección debe ser identificado y ser definido claramente. Estas guías de consulta describen mismo un método conservador para desplegar la protección ACL usando un acercamiento iterativo.

1. **Identifique los protocolos usados en la red con una clasificación ACL.**Despliegue un ACL que permita todos los protocolos conocidos los dispositivos de esa infraestructura de acceso. Esta detección ACL tiene una dirección de origen de **ningunos** y de un destino que abarque el espacio IP de la infraestructura. La registración se puede utilizar para desarrollar una lista de direcciones de origen que correspondan con las declaraciones de permiso de protocolo. Una línea más reciente **IP de** permiso **cualquier** (IPv4) o **IPv6 cualquier** (IPv6) se requiere para permitir el flujo de tráfico.El objetivo es determinar qué protocolos utiliza la red

específica. La registración se utiliza para que el análisis determine qué más pudo comunicar con el router.**Nota:** Aunque la palabra clave del **registro** proporcione el conocimiento valioso en los detalles de los golpes ACL, los golpes excesivos a una entrada ACL que utiliza esta palabra clave pudieron dar lugar a un número impresionante de entradas de registro y posiblemente de alto CPU del router uso. También, usando el **registro la** palabra clave inhabilita el Cisco Express Forwarding (CEF) que conmuta para los paquetes que hacen juego 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. Apenas como en el paso 1, la palabra clave del **registro** puede proporcionar más información sobre los paquetes que hacen juego las entradas del **permiso**. El uso de deny any en el final puede ayudar a identificar cualquier paquete inesperado destinado a los routers. La línea más reciente de este ACL debe ser un **IP cualquier ninguno del permiso** (IPv4) o **permitir que el IPv6 cualquier cualquier** declaración (del IPv6) permita el flujo de tráfico de tránsito. Este ACL proporciona la protección básica y permite que los ingenieros de red se aseguren de que todo el tráfico requerido esté permitido.
3. **Restrinja a 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, usted puede permitir explícitamente los vecinos del BGP externo o a las direcciones de peer específicas GRE.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 a las direcciones destino en el ACL. (*opcional*)**Algunos Proveedores de servicios de Internet (ISP) pudieron elegir permitir solamente que los protocolos específicos utilicen a las direcciones destino específicas en el router. Esta fase final se significa para limitar el rango de las direcciones destino que pueden validar el tráfico para un protocolo.

Ejemplos de despliegue

Ejemplo del IPv4

Este ejemplo del IPv4 muestra una infraestructura ACL que protege a un router basado en esta dirección:

- El bloqueo de dirección ISP es 169.223.0.0/16.
- El bloque de la 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 Protección de la Infraestructura ACL visualizada se desarrolla sobre la base de la información precedente. El ACL permite el BGP externo que mira al peer externo, proporciona los filtros del anti-spoof, y protege la infraestructura contra todo el acceso externo.

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

```
!
! !!!!
```

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