Listas de control de acceso y fragmentos de IP

Contenido

Introducción

Este Informe oficial explica los distintos tipos de entradas de Lista de control de acceso (ACL) y lo que sucede cuando distintas clases de paquetes se enfrentan con diferentes entradas. Las ACL se utilizan para bloquear los paquetes IP reenviados por un router.

RFC 1858 cubre consideraciones de seguridad para el filtrado de fragmentos IP y resalta dos ataques en hosts que involucran fragmentos IP de paquetes TCP, el Ataque de fragmentos pequeños y el Ataque de fragmentos superpuestos. Bloquear estos ataques es deseable porque pueden poner en peligro un host o vincular todos sus recursos internos.

RFC 1858 también describe dos métodos de defensa contra estos ataques, el directo y el indirecto. En el método directo, se descartan los fragmentos iniciales que son menores que una longitud mínima. El método indirecto implica descartar el segundo fragmento de un conjunto de fragmentos, si comienza 8 bytes dentro del datagrama de IP original. Consulte RFC 1858 para obtener más detalles.

Tradicionalmente, los filtros de paquetes como las ACL se aplican a los no fragmentos y al fragmento inicial de un paquete IP porque contienen información de Capa 3 y 4 con la que las ACL pueden coincidir para una decisión de permiso o denegación. Tradicionalmente, los fragmentos no iniciales se permiten a través de la ACL porque se pueden bloquear según la información de la Capa 3 en los paquetes; sin embargo, como estos paquetes no contienen información de Capa 4, no coinciden con la información de Capa 4 en la entrada ACL, si existe. Permitir el paso de los fragmentos no iniciales de un datagrama IP es aceptable porque el host que recibe los fragmentos no puede reensamblar el datagrama IP original sin el fragmento inicial.

Los firewalls también se pueden utilizar para bloquear paquetes mediante el mantenimiento de una tabla de fragmentos de paquetes indexados por dirección IP de origen y destino, protocolo e ID de IP. Tanto el Cisco PIX Firewall como el Cisco IOS® Firewall pueden filtrar todos los fragmentos de un flujo particular manteniendo esta tabla de información, pero es demasiado

costoso hacerlo en un router para la funcionalidad básica de ACL. El trabajo principal de un firewall es bloquear paquetes y su función secundaria es rutear paquetes; La tarea principal de un router es rutear paquetes, y su función secundaria es bloquearlos.

Las versiones del IOS de Cisco 12.1(2) y 12.0(11) introdujeron dos cambios a fin de abordar algunos problemas de seguridad en relación con fragmentos TCP. El método indirecto, como se describe en RFC 1858 , se implementó como parte de la verificación de integridad de paquetes de entrada TCP/IP estándar. También se realizaron cambios en la funcionalidad de ACL con respecto a fragmentos no iniciales.

Tipos de entradas ACL

Existen seis tipos diferentes de líneas de ACL y cada uno tiene una consecuencia si un paquete coincide o no. En la siguiente lista, FO = 0 indica un fragmento no-fragmento o un fragmento inicial en un flujo TCP, FO > 0 indica que el paquete es un fragmento no inicial, L3 significa Capa 3 y L4 significa Capa 4.

Nota: Cuando hay información de Capa 3 y Capa 4 en la línea ACL y la palabra clave **fragments** está presente, la acción ACL es conservadora para las acciones permit y deny. Las acciones son conservadoras por que no deseará negar accidentalmente una porción fragmentada de un flujo porque los fragmentos no contienen la información necesaria para coincidir con todos los atributos del filtro. En el caso deny, en lugar de negar un fragmento no inicial, se procesa la siguiente entrada ACL. En el caso permit, se asume que la información de Capa 4 en el paquete, si está disponible, coincide con la información de Capa 4 en la línea ACL.

Autorizar la línea ACL sólo con información de L3.

1. Si la información L3 de un paquete coincide con la información L3 en la línea ACL, se permite.
2. Si la información de L3 de un paquete no concuerda con la información de L3 en la línea ACL, se procesa la siguiente entrada ACL.

Rechazar la línea ACL sólo con información L3.

1. Si la información de un paquete L3 coincide con la información L3 en la línea ACL, se la deniega.
2. Si la información de L3 de un paquete no concuerda con la información de L3 en la línea ACL, se procesa la siguiente entrada ACL.

Permitir la línea ACL sólo con información de L3 y la palabra clave fragments está presente

Si la información L3 de un paquete coincide con la información L3 en la línea ACL, se verifica el desplazamiento del fragmento del paquete.

1. Si un paquete es FO > 0, el paquete está permitido.
2. Si el FO de un paquete = 0, se procesa la siguiente entrada de ACL.

Denegar la línea ACL sólo con información de L3 y la palabra clave fragments está presente

Si la información de L3 de un paquete coincide con la información de L3 en la línea ACL, se verifica el desplazamiento del fragmento del paquete.

1. Si el FO de un paquete es > 0, el paquete está denegado.
2. Si el FO de un paquete es igual a 0, se procesa la siguiente línea ACL.

Permitir la línea ACL con información de las capas 3 y 4

1. Si la información L3 y L4 de un paquete coincide con la línea ACL y FO = 0, se permite el paquete.
2. Si la información de L3 de un paquete coincide con la línea de la ACL y FO > 0, el paquete está permitido.

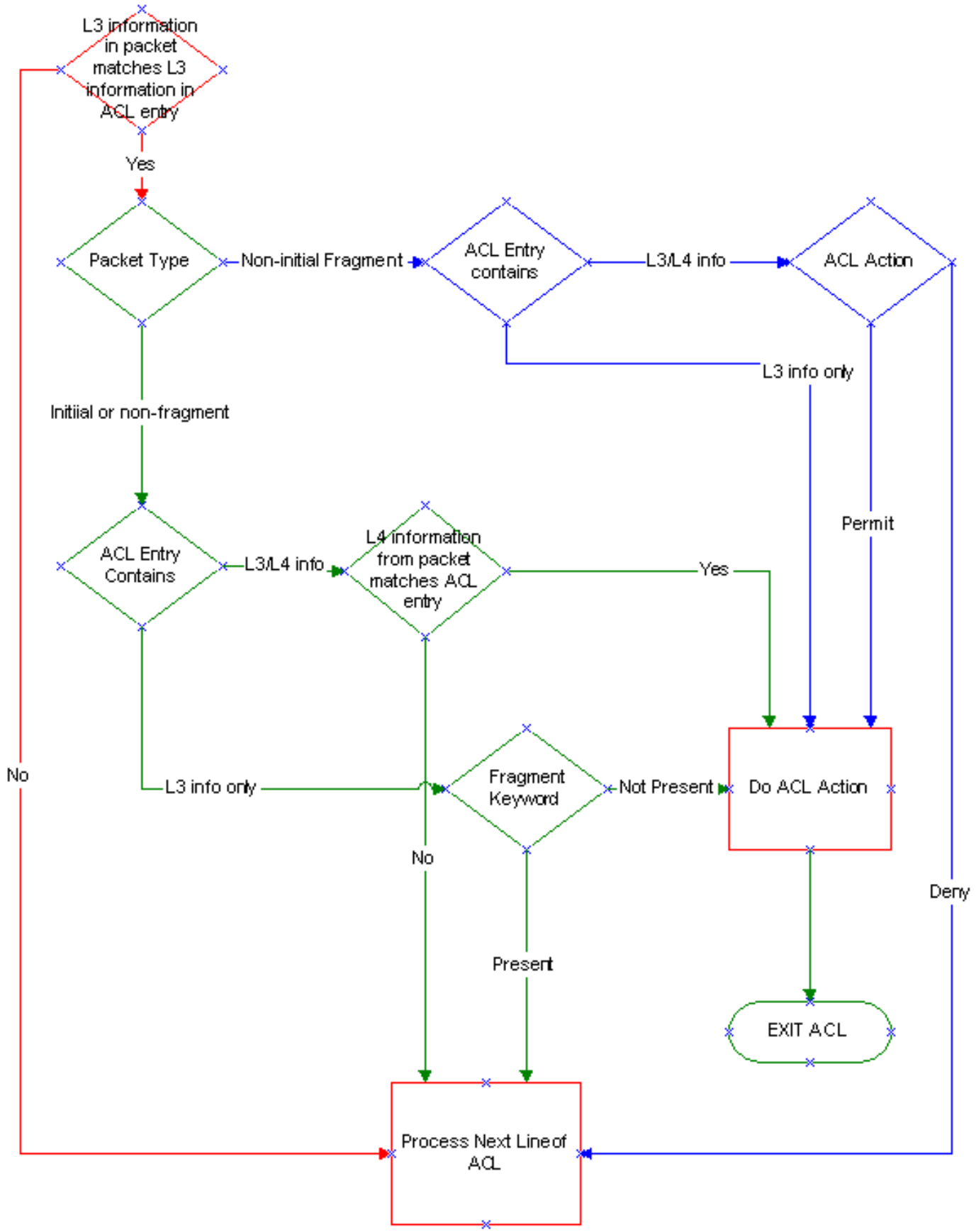
Deniegue la línea ACL con información de las capas 3 y 4

1. Si la información L3 y L4 de un paquete coincide con la entrada ACL y FO = 0, el paquete se niega.
2. Si la información L3 de un paquete coincide con la línea ACL y FO > 0, se procesa la siguiente entrada ACL.

Diagrama de flujo de las reglas ACL

El siguiente organigrama ilustra las normas sobre ACL que se utilizan al comparar no fragmentos, fragmentos iniciales y fragmentos no iniciales con la ACL.

Nota: Los fragmentos no iniciales contienen solamente información de Capa 3, nunca de Capa 4, aunque la ACL puede contener información de Capa 3 y Capa 4.



Cómo los paquetes pueden coincidir con una ACL

Ejemplo 1

Los siguientes cinco escenarios posibles involucran diferentes tipos de paquetes que se

encuentran con ACL 100. Consulte la tabla y el diagrama de flujo mientras sigue lo que sucede en cada situación. La dirección IP del servidor Web es 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

El paquete es un fragmento inicial o un no fragmento destinado al servidor en el puerto 80:

La primera línea de la ACL contiene información de Capa 3 y Capa 4, que coincide con la información de Capa 3 y Capa 4 en el paquete, por lo que se permite el paquete.

El paquete es un fragmento inicial o sin fragmento destinado para el servidor en el puerto 21.

1. La primera línea de la ACL contiene información de Capa 3 y Capa 4, pero la información de Capa 4 en la ACL no coincide con el paquete, por lo que se procesa la siguiente línea ACL.
2. La segunda línea de la ACL deniega a todos los paquetes, de modo que el paquete es denegado.

El paquete es un fragmento no inicial en el servidor en el flujo de un puerto 80:

La primera línea de la ACL contiene información de capa 3 y capa 4, la información de capa 3 en la ACL coincide con el paquete, la acción de la ACL es permitir, de manera que el paquete sea permitido.

El paquete es un fragmento no inicial al servidor en un flujo de puerto 21:

La primera línea de la ACL contiene información de la capa 3 y la capa 4. La información de la capa 3 en el ACL coincide con el paquete, no existe información de la capa 4 en el paquete y la acción del ACL es permitir y, por lo tanto, el paquete es permitido.

El paquete es un fragmento inicial, no es un fragmento o no es un fragmento inicial de otro host en la subred del servidor:

1. La primera línea de la ACL incluye la información de la Capa 3 que no coincide con la información de la Capa 3 en el paquete (la dirección de destino), por esta razón, se procesa la próxima línea de la ACL.
2. La segunda línea de la ACL deniega a todos los paquetes, de modo que el paquete es denegado.

Ejemplo 2

Los siguientes cinco escenarios posibles implican diferentes tipos de paquetes que se encuentran con ACL 101. De nuevo, consulte la tabla y el diagrama de flujo a medida que siga lo que sucede en cada situación. La dirección IP del servidor Web es 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

El paquete es un fragmento inicial o no un fragmento destinado al servidor en el puerto 80:

1. La primera línea de ACL contiene información de Capa 3 que coincide con la información de Capa 3 del paquete. La acción ACL es denegar, pero debido a que la palabra clave **fragments** está presente, se procesa la siguiente entrada ACL.
2. La segunda línea de la ACL contiene información de la Capa 3 y de la Capa 4 la cual coincide con el paquete, por lo tanto el paquete es permitido.

El paquete es un fragmento inicial o no un fragmento destinado al servidor en el puerto 21:

1. La primera línea de la ACL contiene información de la Capa 3, que coincide con el paquete, pero la entrada de la ACL también tiene la palabra clave **fragments**, que no coincide con el paquete porque FO = 0, por lo que se procesa la siguiente entrada de ACL.
2. La segunda línea de la ACL contiene información de la capa 3 y la capa 4. En este caso, la información de la Capa 4 no coincide, por lo que se procesa la siguiente entrada ACL.
3. La tercera línea del ACL deniega todos los paquetes; por lo tanto, el paquete es denegado

El paquete es un fragmento no inicial en el servidor en el flujo de un puerto 80:

La primera línea de ACL contiene información de Capa 3 que coincide con la información de Capa 3 del paquete. Recuerde que aunque esto es parte del flujo de un puerto 80, no existe información de Capa 4 en el fragmento no inicial. El paquete se niega porque la información de la Capa 3 coincide.

El paquete es un fragmento no inicial al servidor en un flujo de puerto 21:

La primera línea de la ACL sólo contiene información de la Capa 3 y coincide con el paquete, por lo tanto el paquete es denegado.

El paquete es un fragmento inicial, no es un fragmento o no es un fragmento inicial de otro host en la subred del servidor:

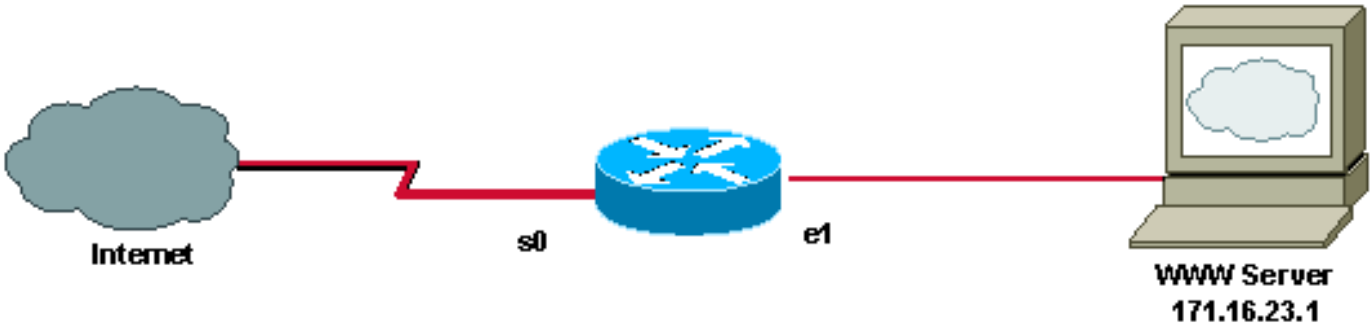
1. La primera línea de la ACL contiene sólo información de capa 3, y no coincide con el paquete, de manera que se procesa la línea siguiente de la ACL.
2. La segunda línea de la ACL contiene información de la capa 3 y la capa 4. La información de Capa 4 y Capa 3 en el paquete no coincide con la de la ACL, por lo que se procesa la siguiente línea ACL.
3. La tercera línea de la ACL niega este paquete

Situaciones de ejemplo de palabras clave de fragmentos

Escenario 1

El router B se conecta a un servidor web y el administrador de red no desea permitir que ningún fragmento llegue al servidor. Este escenario muestra lo que sucede si el administrador de la red implementa ACL 100 frente a ACL 101. La ACL se aplica de forma entrante en la interfaz Serial0 (s0) de los routers y sólo debe permitir que los paquetes no fragmentados lleguen al servidor web. Consulte el diagrama de flujo de reglas de ACL y las secciones Cómo los paquetes pueden coincidir con una ACL mientras sigue la situación.

Consecuencias de la utilización de la palabra clave fragmentos



La siguiente es la ACL 100:

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

La primera línea de la ACL 100 permite únicamente el HTTP al servidor, pero también admite los fragmentos no iniciales a cualquier puerto del TCP en el servidor. Permite estos paquetes porque los fragmentos no iniciales no contienen información de la Capa 4, y la lógica ACL asume que si la información de la Capa 3 coincide, la información de la Capa 4 también coincidiría, si estuviera disponible. La segunda línea es implícita y niega todo el otro tráfico.

Es importante tener en cuenta que, a partir de las versiones 12.1(2) y 12.0(11) del software del IOS de Cisco, el nuevo código ACL descarta fragmentos que no coinciden con ninguna otra línea en la ACL. Las versiones anteriores permiten fragmentos no iniciales a través si no coinciden con ninguna otra línea de la ACL.

El siguiente es ACL 101:

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

La ACL 101 no permite que pasen fragmentos no iniciales al servidor debido a la primera línea. Se niega un fragmento no inicial al servidor cuando encuentra la primera línea ACL porque la información de Capa 3 en el paquete coincide con la información de Capa 3 en la línea ACL.

Los fragmentos iniciales o no del puerto 80 en el servidor también coinciden con la primera línea de la ACL para la información de la Capa 3, pero como la palabra clave fragments está presente, se procesa la siguiente entrada ACL (la segunda línea). La segunda línea de la ACL permite los fragmentos iniciales o no iniciales porque concuerdan con la línea ACL para la información de las Capas 3 y 4.

Los fragmentos no iniciales destinados a los puertos TCP de otros hosts en la red 171.16.23.0 están bloqueados por esta ACL. La información de la Capa 3 en estos paquetes no coincide con la información de la Capa 3 en la primera línea ACL, entonces se procesa la siguiente línea ACL. La información de Capa 3 en estos paquetes tampoco coincide con la información de Capa 3 en la segunda línea ACL, por lo tanto se procesa la tercera línea ACL. La tercera línea está implícita y niega todo el tráfico.

El administrador de la red en este escenario decide implementar ACL 101 porque permite que sólo los flujos HTTP no fragmentados ingresen en el servidor.

Escenario 2

Un cliente tiene conectividad a Internet en dos sitios diferentes, y también hay una conexión de puerta trasera entre los dos sitios. La política del administrador de la red es permitir que el Grupo A en el Sitio 1 acceda al servidor HTTP en el Sitio 2. Los routers en ambos sitios utilizan direcciones privadas (RFC 1918) y traducción de direcciones de red (NAT) para traducir paquetes que se enrutan a través de Internet.

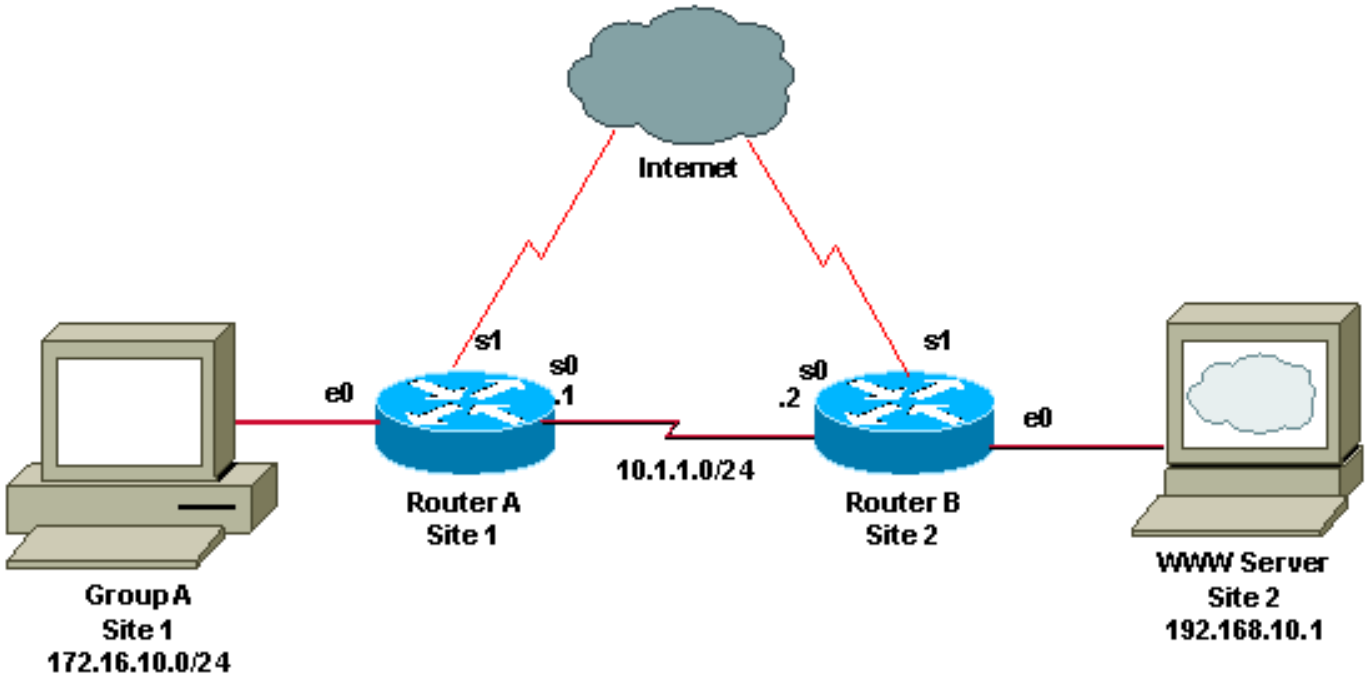
El administrador de la red en el Sitio 1 está ruteando las direcciones privadas asignadas al Grupo A, de modo que utilicen la puerta trasera a través del Serial0 (s0) del Router A al acceder al servidor HTTP en el Sitio 2. El router en el Sitio 2 tiene una ruta estática a 172.16.10.0, de modo que el tráfico de retorno al Grupo A también se rutea a través de la puerta trasera. El resto del tráfico es procesado por NAT y ruteado a través de Internet. En este escenario, el administrador de red debe decidir qué aplicación o qué flujo funcionará si se fragmentan los paquetes. No es posible hacer que los flujos HTTP y FTP funcionen al mismo tiempo porque uno o los otros se interrumpirán.

Consulte el diagrama de flujo de reglas de ACL y las secciones Cómo los paquetes pueden coincidir con una ACL mientras sigue la situación.

Explicación de las opciones del administrador de red

En el siguiente ejemplo, el route map llamado FOO en el Router A envía paquetes que coinciden con ACL 100 a través del Router B a través de s0. Todos los paquetes que no coinciden son procesados por NAT y toman la ruta predeterminada a través de Internet.

Nota: Si un paquete cae de la parte inferior de la ACL o es denegado por ella, no se rutea mediante políticas.



La siguiente es una configuración parcial del Router A, que muestra que se aplica un mapa de ruta de política llamado FOO a la interfaz e0, donde el tráfico del Grupo A ingresa al router:

```
hostname Router_A
int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

La ACL 100 permite el ruteo de políticas tanto en fragmentos iniciales, sin fragmentos como no iniciales de flujos HTTP al servidor. La ACL y la política ruteadas permiten los flujos HTTP iniciales y no fragmentos al servidor porque coinciden con la información de Capa 3 y Capa 4 en la primera línea ACL. La ACL permite fragmentos no iniciales y la política ruteada porque la información de Capa 3 en el paquete también coincide con la primera línea ACL; la lógica ACL asume que la información de la Capa 4 en el paquete también coincidiría si estuviera disponible.

Nota: ACL 100 rompe otros tipos de flujos TCP fragmentados entre el Grupo A y el servidor porque los fragmentos inicial y no inicial llegan al servidor a través de diferentes trayectorias; los fragmentos iniciales son procesados por NAT y ruteados a través de Internet, pero los fragmentos no iniciales del mismo flujo son ruteados por políticas.

Un flujo FTP fragmentado ayuda a ilustrar el problema en este escenario. Los fragmentos iniciales de un flujo FTP coinciden con la información de la Capa 3 pero no con la información de la Capa 4 de la primera línea ACL y posteriormente son denegados por la segunda línea. Estos paquetes son procesados por NAT y enrutados a través de Internet.

Los fragmentos no iniciales de un flujo FTP coinciden con la información de Capa 3 en la primera línea ACL, y la lógica ACL asume una coincidencia positiva en la información de Capa 4. Estos paquetes están enrutados por política, y el host que reensambla estos paquetes no reconoce los

fragmentos iniciales como parte del mismo flujo que los fragmentos no iniciales enrutados por política porque NAT ha cambiado la dirección de origen de los fragmentos iniciales.

La ACL 100 en la siguiente configuración corrige el problema de FTP. La primera línea de ACL 100 niega los fragmentos FTP iniciales y no iniciales del Grupo A al servidor.

```
hostname Router_A

int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 fragments
access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

Los fragmentos iniciales coinciden en la información de Capa 3 en la primera línea ACL, pero la presencia de la palabra clave **fragments** hace que se procese la siguiente línea ACL. El fragmento inicial no coincide con la segunda línea ACL para la información de la Capa 4, por lo que se procesa la siguiente línea implícita de la ACL, que niega el paquete. Los fragmentos no iniciales coinciden con la información de Capa 3 en la primera línea de la ACL, por lo que se niegan. NAT procesa los fragmentos iniciales y no iniciales y los rutea a través de Internet, por lo que el servidor no tiene problema con el reensamblado.

La corrección de los flujos FTP interrumpe los flujos HTTP fragmentados porque los fragmentos HTTP iniciales ahora se enrutan mediante políticas, pero NAT procesa los fragmentos no iniciales y se enrutan a través de Internet.

Cuando un fragmento inicial de un flujo HTTP del Grupo A al servidor se enfrenta con la primera línea del ACL, coincide con la información de Capa 3 en el ACL, pero debido a la palabra clave fragments, se procesa la siguiente línea del ACL. La segunda línea de la ACL permite y la política enruta el paquete al servidor.

Cuando los fragmentos HTTP no iniciales destinados desde el Grupo A al servidor se enfrentan con la primera línea del ACL, la información de Capa 3 en el paquete coincide con la línea ACL y se rechaza el paquete. NAT procesa estos paquetes que atraviesan Internet para llegar al servidor.

La primera ACL en este escenario permite flujos HTTP fragmentados y rompe flujos FTP fragmentados. La segunda ACL permite los flujos fragmentados de FRP e interrumpe los flujos fragmentados de HTTP. Los flujos de TCP se interrumpen en cada caso porque los fragmentos iniciales y no iniciales toman diferentes trayectos hacia el servidor. El reensamblado no es posible porque NAT cambió la dirección de origen de los fragmentos no iniciales.

No es posible construir una ACL que permita ambos tipos de flujos fragmentados hacia el servidor, entonces el administrador de red debe elegir con qué flujo quiere trabajar.

Información Relacionada

- Página de Soporte de IP Routing

- Soporte Técnico y Documentación - Cisco Systems