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 (GRS) se pueden dividir en dos categorías generales:

- Trafique que los pasos a través del router vía el trayecto de reenvío.
- Trafique que se debe enviar vía la trayectoria de la recepción al GRP para el análisis adicional.

En los funcionamientos normales, el amplia mayoría de tráfico atraviesa simplemente un GSR en el camino a otros destinos. Sin embargo, el GRP debe manejar los tipos determinados de datos, especialmente los Routing Protocol, acceso del router remoto, y tráfico de administración de red (tal como protocolo administración de red simple [SNMP]). Además de este tráfico, otro los paquetes de la capa 3 pudo requerir la flexibilidad de proceso del GRP. Éstos incluirían ciertas opciones IP y ciertas formas de paquetes del Internet Control Message Protocol (ICMP). Refiera al apéndice encendido reciben las adyacencias y los paquetes llevados en batea para los detalles adicionales con respecto al rACLs y reciben el tráfico de la trayectoria en el GSR.

Un GSR tiene varios trayectos de datos, cada diversas formas de mantenimiento 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 del trayecto de datos del tráfico de tránsito, un GSR tiene dos otras trayectorias para el tráfico que requiere el

procesamiento local: LC a LC CPU y al LC a LC CPU a la tela al GRP. La tabla que se muestra a continuación ilustra los trayectos para las características y los protocolos generalmente utilizados.

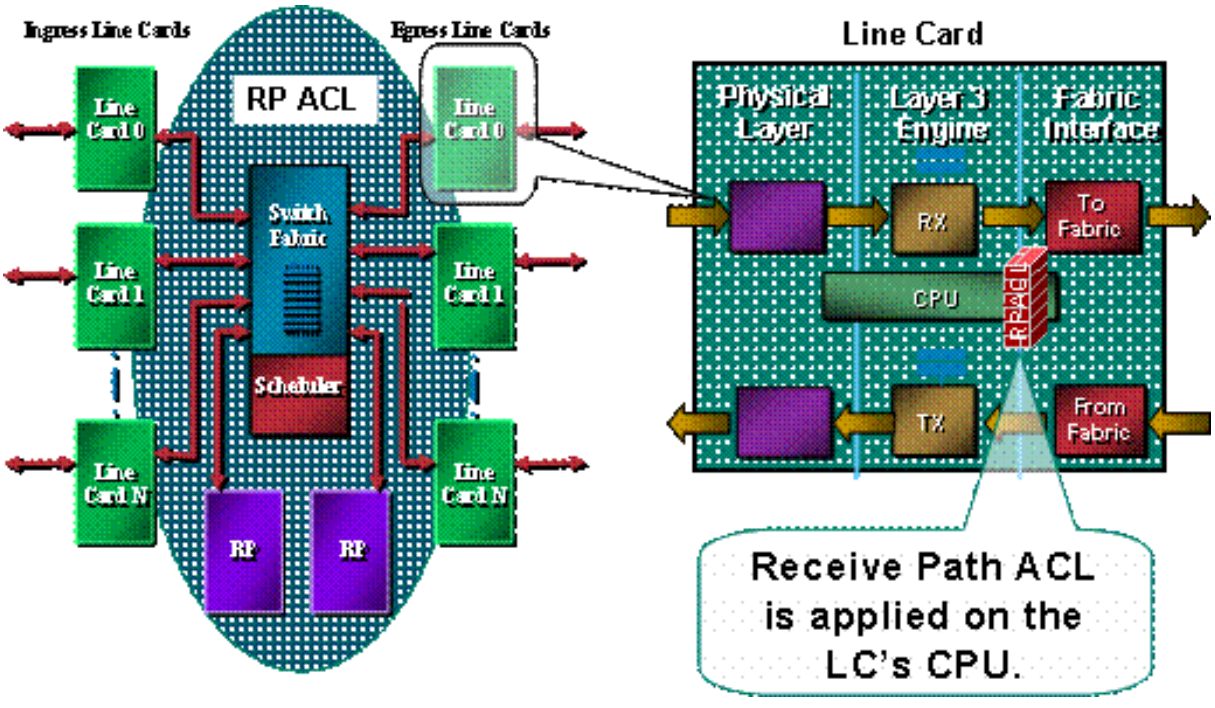
'Tipo de tráfico'	Trayecto de datos
(Transite) tráfico normal	LC a la tela al LC
Rutear Protocols/SSH/SNMP	LC a LC CPU a la tela al GRP
Eco ICMP (ping)	LC a LC CPU
Registro	

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 volumen alto de datos requiere llevar en batea al GRP, ese tráfico puede abrumar el GRP. Esto da lugar a un ataque de Negación de servicio (DoS) eficaz. El CPU del GRP lucha para continuar con el examen del paquete y comienza a caer los paquetes, inundando el entrada-control y las colas de administración del tráfico del Selective Packet Discard (SPD). [2] GSR se deben proteger contra tres escenarios, que pueden resultar de los ataques DOS dirigidos en un GRP del router.

- Pérdida del paquete del Routing Protocol de una inundación de la prioridad normal
- Pérdida del paquete de la Sesión de administración (Telnet, shell seguro [SSH], SNMP) de una inundación de la prioridad normal
- Pérdida de paquete de una inundación de alta prioridad simulada

La pérdida potencial de datos del Routing Protocol durante una inundación de la prioridad normal es paliada actualmente por la clasificación estática y la limitación de la tarifa del tráfico destinada al GRP de los LC. Desafortunadamente, este enfoque tiene limitaciones. La tarifa que limita para el tráfico de la prioridad normal destinado al GRP es escasa para garantizar la protección a los datos prioritarios del Routing Protocol si un ataque se entrega vía varios LC. Bajando el umbral en el cual los datos de la prioridad normal se caen para proporcionar tal protección exacerba solamente la pérdida de tráfico de administración de una inundación de la prioridad normal.

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



Un mecanismo de protección para el GRP se requiere. el tráfico de la influencia del rACLs debido al cual se envía al GRP recibe las adyacencias. Reciba las adyacencias son adyacencias del Cisco Express Forwarding para el tráfico destinado a los IP Addresses del router, tales como la dirección de broadcast o los direccionamientos configurados en las interfaces del router. [3] vea la sección del apéndice para más detalles encendido recibir las adyacencias y los paquetes llevados en batea.

Trafique que ingresa un LC primero se envía al CPU local del LC, y los paquetes que requieren el proceso por el GRP se hacen cola para remitir al Route Processor. 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 del LC CPU al GRP, el tráfico se compara al rACL. Si está permitido, el tráfico pasa al GRP, mientras que se niega el resto del tráfico. 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.

Reciba los ACL son parte uno de una variedad de mecanismos de un programa de varias partes para proteger los recursos en un router. El trabajo futuro incluirá un componente de la limitación de la tarifa al rACL.

Impacto en el rendimiento

No se consume ninguna memoria con excepción de ése necesario llevar a cabo la sola entrada de configuración y la lista de acceso definida sí mismo. El rACL se copia a cada LC, así que una área de memoria leve se toma en cada LC. Totales, los recursos utilizados son minúsculos, especialmente en comparación con las ventajas del despliegue.

Una recepción ACL no afecta al funcionamiento del tráfico remitido. El rACL se aplica solamente para recibir el tráfico de la adyacencia. El tráfico remitido nunca está conforme al rACL. El tráfico de tránsito se filtra con ACL de interfaz. ¿Éstos? ¿regular? Los ACL se aplican a las interfaces en una dirección especificada. El tráfico está conforme a procesamiento ACL antes de procesamiento rACL, así que el tráfico negado por la interfaz ACL no será recibido por el rACL. [4]

El LC que realiza la filtración real (es decir el LC que recibe el tráfico filtrado por el rACL) tendrá utilización de la CPU incrementada debido al proceso del rACL. Esta utilización de la CPU incrementada, sin embargo, es causada por un volumen alto de tráfico destinado al GRP; la ventaja del GRP de la protección rACL sobrepasa lejos la utilización de la CPU incrementada en un LC. El uso de la CPU en una LC varía de acuerdo al tipo de motor de LC. Por ejemplo, dado el mismo ataque, Motor 3 un LC tendrá utilización de la CPU más baja que un motor 0 LC.

Habilitar turbo ACL (usando el **comando access-list compiled**) convierte los ACL en una serie muy eficiente de entradas de tabla de las operaciones de búsqueda. Cuando se habilita turbo ACL, la profundidad rACL no afecta al funcionamiento. Es decir la velocidad de procesamiento es independiente del número de entradas en el ACL. Si el rACL es corto, turbo ACL no aumentará perceptiblemente el funcionamiento sino consumirá la memoria; con el rACLs corto, los ACL compilados son no necesarios probable.

Protegiendo el GRP, las ayudas del rACL aseguran el router y, en última instancia, la estabilidad de la red durante un ataque. Como se describe anteriormente, el rACL se procesa en el LC CPU, así que la utilización de la CPU en cada LC aumentará cuando un de gran capacidad de los datos se dirige en el router. En el E0/E1 y algunos conjuntos E2, la utilización de la CPU del 100+% pudo llevar a los descensos del Routing Protocol y de la 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. Los indicadores luminosos LED amarillo de la placa muestra gravedad menor E2 con el microcódigo estrangular-habilitado [5] activan al modo de descenso del multiplicador cuando bajo la carga pesada y solamente precedencia delantera 6 y el tráfico 7 al Routing Protocol. Otros tipos de motor tienen arquitecturas de la multi-cola; por ejemplo, los indicadores luminosos LED amarillo de la placa muestra gravedad menor E3 tienen tres colas de administración del tráfico al CPU, con los paquetes del Routing Protocol (precedencia 6/7) en un separado, cola de alta prioridad. El alto LC CPU, a menos que los paquetes de alta precedencia lo causen, no dará lugar a los descensos del Routing Protocol. Los paquetes a las colas de menor prioridad Tail-serán caídos. Finalmente, los indicadores luminosos LED amarillo de la placa muestra gravedad menor E4-based tienen ocho colas de administración del tráfico al CPU, con uno dedicado a los paquetes del Routing Protocol.

Sintaxis

Una recepción ACL se aplica con el comando global configuration siguiente de distribuir el rACL a cada LC en el router.

[no] ip receive access-list *<num>*

En este sintaxis, el ***<num>*** se define como sigue.

[no] ip receive access-list *<num>*

Plantilla básica y Ejemplos de ACL

Para poder utilizar este comando, usted necesita definir una lista de acceso que identifique el tráfico que se debe permitir hablar 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 el SNMP, un Loopback Address se utiliza como el destino. Para los Routing Protocol, se utiliza el direccionamiento real de la interfaz. La elección de interfaces de router que se utilizará en la rACL está determinada por políticas y operaciones del sitio local. Por ejemplo, si los loopback se utilizan para todas las sesiones de peer BGP, después solamente esos loopback necesitan ser permitidos en las declaraciones del **permiso** para el BGP.

[no] ip receive access-list *<num>*

Como con todo el Cisco ACL, hay un **enunciado de negación** implícito en el extremo de la lista de acceso, tan cualquier tráfico que no haga juego una entrada en el ACL sea negado.

Nota: La palabra clave del **registro** se puede utilizar para ayudar a clasificar el tráfico destinado al GRP que no se permite. 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 utilice esta palabra clave aumentarán la utilización de la CPU LC. El impacto del rendimiento asociado al registro variará con el tipo de motor LC. Generalmente la registración se debe utilizar solamente cuando sea necesario en los motores 0/1/2. Para los motores 3/4/4+, la registración resulta adentro lejos menos de un impacto debido al funcionamiento de la CPU incrementada y la arquitectura de la multi-cola.

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

Los ACL tienen una palabra clave de los **fragmentos** que habilite el comportamiento hecho fragmentos especializado de la dirección del paquete. Los fragmentos no iniciales que hacen juego las declaraciones L3 (con independencia de la información L4) en un ACL son afectados generalmente por la declaración del **permit or deny de la** entrada correspondida con. Observe que el uso de la palabra clave de los **fragmentos** puede forzar los ACL a niega o permite los fragmentos no iniciales con más granularity.

En el contexto rACL, la filtración de los fragmentos agrega una capa adicional de protección contra un ataque DOS que utilice solamente los fragmentos no iniciales (por ejemplo 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. Bajo circunstancias poco probables, una sesión válida pudo requerir la fragmentación y por lo tanto ser filtrado si una declaración del **fragmento de la negación** existe en el rACL.

Por ejemplo, considere el ACL parcial mostrado abajo.

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

Agregar estas entradas al principio de un rACL niega cualquier acceso del fragmento no inicial al GRP, mientras que los paquetes no fragmentados o los fragmentos iniciales pasan a las líneas siguientes del rACL inafectado por las declaraciones del **fragmento de la negación**. ¿Los fragmentos de rACL antedichos también facilitan la clasificación del ataque desde cada protocolo? ¿Datagram Protocol universal (UDP), TCP, y ICMP? los incrementos separan los contadores en el ACL.

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

Evaluación de riesgo

Asegúrese de que el rACL no filtre el tráfico crítico tal como Routing Protocol o acceso interactivo al Routers. El tráfico necesario de filtración podía dar lugar a una incapacidad para acceder remotamente al router, así requiriendo una conexión de consola. Por este motivo, las configuraciones de laboratorio deben imitar el despliegue real lo más posible.

Como siempre, Cisco recomienda que usted prueba esta característica en el laboratorio antes del despliegue.

Apéndices y notas

Recibir adyacencias y paquetes liberados

Según lo descrito anterior en este documento, algunos paquetes requieren el procesamiento GRP. Los paquetes son impulsados desde el plano de reenvío de datos hacia el GRP. Ésta es una lista de las formas comunes de datos de la capa 3 que requieran el acceso GRP.

- Protocolos de ruteo
- Tráfico de control de multidifusión (OSPF, protocolo del router de la espera en caliente [HSRP], Tag Distribution Protocol [TDP], multidifusión independiente de protocolo [PIM], y tal)
- Paquetes del Multiprotocol Label Switching (MPLS) que necesitan la fragmentación
- Paquetes con ciertas opciones IP, como por ejemplo alerta del router.
- Primer paquete de secuencias de multidifusión
- Paquetes icmp hechos fragmentos que requieren el nuevo ensamble
- Todos trafican destinado al router sí mismo (a excepción del tráfico manejado en el LC)

Puesto que el rACLs se aplica para recibir las adyacencias, el rACL filtra un cierto tráfico que no se lleve en batea al GRP pero es una adyacencia de la recepción. El ejemplo más común de esto es una petición de eco ICMP (ping). Los pedidos de eco ICMP dirigidos al router son manejados por el LC CPU; puesto que son las peticiones reciba las adyacencias, ellas también son filtrados por el 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 cefPrefix              Next Hop             Interface0.0.0.0/0           drop
Null0 (default route handler entry)1.1.1.1/32          attached             Null02.2.2.2/32
receive64.0.0.0/30         attached             ATM4/3.300...
```

Pautas para la instrumentación

Cisco recomienda las prácticas conservadoras del despliegue. Para desplegar con éxito el rACLs, los requisitos existentes del control y del acceso del plano de administración deben ser entendidos bien. En algunas redes, determinar el perfil del tráfico exacto necesario para construir las listas de filtración pudo ser difícil. 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 usados en la red con una clasificación ACL.**Despliegue un rACL que permite todos los protocolos conocidos que acceden el GRP. ¿Esto? ¿detección? el rACL debe tener ambo las direcciones de origen y de destino fijadas a **ningunos**. La registración se puede utilizar para desarrollar una lista de direcciones de origen que correspondan con las declaraciones de permiso de protocolo. Además de la declaración de permiso de protocolo, un **permiso cualquier cualquier línea del registro** en el final del rACL se puede utilizar para identificar otros protocolos que serían filtrados por el rACL y que pudieron requerir el acceso al GRP.El objetivo es determinar qué protocolos utiliza la red específica. ¿La registración se debe utilizar 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. 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. 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 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 los protocolos que necesitan comunicar con el router sin tener el rango explícito del IP de origen y de las direcciones destino.
3. **Restrinja un rango macro de las 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 le han afectado un aparato 171.68.0.0/16 para su red, después permita a las direcciones de origen de apenas 171.68.0.0/16.Este paso minimiza el riesgo sin interrumpir ningún servicio. También proporciona los puntos de datos de los dispositivos/de gente fuera de su bloque CIDR que pudo acceder su equipo. Caerán a toda la dirección externa.Los pares del BGP externo requerirán una excepción, puesto que los direccionamientos de fuente permitida para la sesión mentirán fuera del bloque CIDR.Esta fase puede dejarse por unos días para que recolecte datos para la siguiente fase de restricción de rACL.
4. **Estreche las declaraciones de permiso rACL para permitir solamente a las direcciones de origen autorizadas conocidas.**Limite cada vez más a la dirección de origen para permitir solamente las fuentes que comunican con el GRP.
5. **Limite a las direcciones destino en el 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 despliegue

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 la 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.

Dado esta información, la inicial recibe el ACL podría ser algo como el ejemplo abajo. Ya que se conoce el bloque de dirección de infraestructura, en un principio se permitirá el bloque completo. Más adelante, entradas de control de acceso más detalladas (ACE) serán agregadas como las direcciones específicas se obtienen para todos los dispositivos que necesitan el 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 224.0.0.6access-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
224.0.0.10access-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 22access-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 1433access-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 65535access-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 más información con respecto el Cisco Express Forwarding y a las adyacencias, refiera a la descripción del Cisco Express Forwarding.
3. Para una explicación detallada de las Pautas para la instrumentación y de los Comandos relacionados ACL, refiere a implementar los ACL en los Cisco 12000 Series Internet Router.
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 trayecto de la 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**