Listas de control de acceso de tránsito: Filtración en su borde

Contenido

Introducción

Este documento incluye pautas y técnicas de instrumentación recomendadas para filtrar el tránsito y limitar el tráfico en sus puntos de ingreso a la red. Las listas de control de acceso de tránsito (ACL) se utilizan para aumentar la seguridad de la red permitiendo explícitamente únicamente el tráfico requerido en la red o redes.

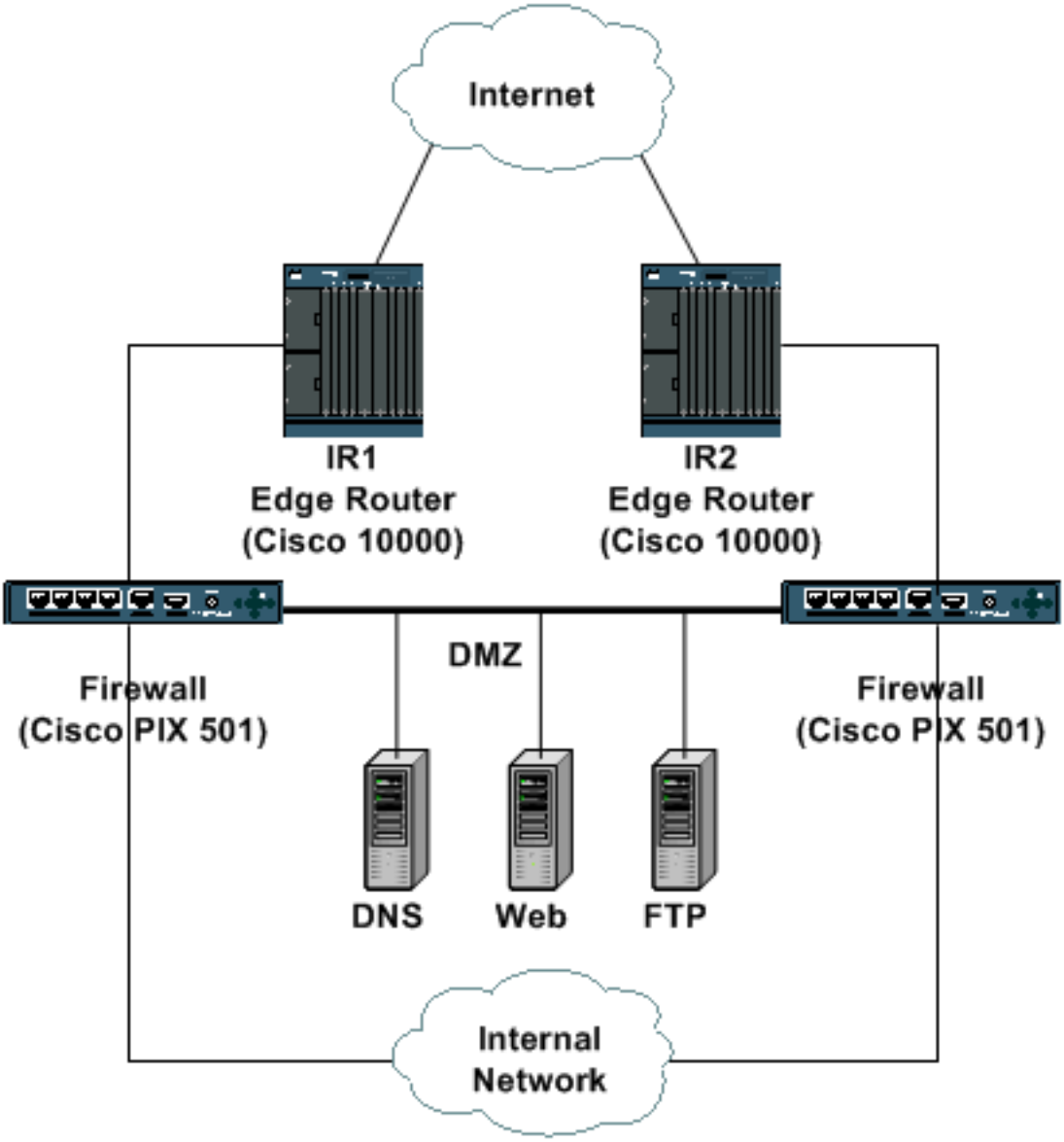
Filtros de tránsito

Configuración típica

En la mayoría de los entornos de red de borde, tales como un Point of Presence del Internet de red de la empresa típica, el filtrado de ingreso se debe utilizar para caer el tráfico desautorizado en el borde de la red. En ciertas implementaciones del proveedor de servicio, esta forma de filtración del borde o del tráfico de tránsito se puede también utilizar eficazmente para limitar el flujo de tráfico de tránsito a y desde los clientes a los protocolos permitidos específico solamente. Este documento se centra sobre un modelo de instrumentación para empresas.

Este ejemplo representa un diseño de la conectividad a Internet de la empresa típica. Dos routeres de borde, IR1 y IR2, proporcionan la conectividad directa a Internet. Detrás de este dos

Routers, un par de los Firewall (PIXes de Cisco en este ejemplo) proporciona las capacidades y el acceso de la inspección con estado a la red interna y a la zona desmilitarizada (DMZ). El DMZ contiene los servicios del público-revestimiento tales como DNS y red; ésta es la única red accesible directamente del Internet pública. Nunca se debe obtener acceso a la red interna directamente por Internet, pero el tráfico de origen de la red interna debe poder llegar a los sitios de Internet.



Los routers de borde deberían estar configurados para ofrecer un primer nivel de seguridad a través del uso de los ACL de entrada. Los ACL permiten solamente específicamente el tráfico permitido al DMZ y permiten el tráfico de retorno para los usuarios internos que acceden Internet. Todo el tráfico nonauthorized se debe caer en las interfaces de ingreso.

Secciones ACL de tránsito

Un transitar ACL se compone generalmente de cuatro secciones.

- Entradas de antisimulación y dirección de uso especial que impiden que fuentes ilegítimas y paquetes con direcciones de origen que pertenecen a su red ingresen a la red desde una fuente externa**Nota:** RFC 1918 define un espacio de dirección reservada que no es una dirección de origen válida en Internet. RFC 3330 define direcciones de uso especial que

pueden requerir filtrado. El RFC 2827 proporciona las guías de consulta contra spoofing.
- Tráfico de retorno explícitamente permitido para las conexiones internas a Internet
- Tráfico externamente originado explícitamente permitido destinado a las direcciones internas protegidas
- **Enunciado de negación** explícito**Nota:** Aunque todos los ACL contengan un **enunciado de negación** implícito, Cisco recomienda el uso de un **enunciado de negación** explícito, por ejemplo, **deny ip any any**. En la mayoría de las plataformas, esas sentencias mantienen un conteo de la cantidad de paquetes denegados que pueden mostrarse utilizando el comando show access-list.

Cómo desarrollar un transitar ACL

El primer paso en el desarrollo de un transitar ACL es determinar los protocolos requeridos dentro de sus redes. Aunque cada sitio tenga requisitos específicos, los ciertos protocolos y aplicaciones son ampliamente utilizados y se permiten lo más a menudo posible. Por ejemplo, si el segmento DMZ proporciona la Conectividad para un servidor Web público accesible, el TCP de Internet al direccionamiento del servidor DMZ en el puerto 80 se requiere. Semejantemente, las conexiones internas a Internet requieren que la vuelta del permiso ACL estableciera tráfico TCP – trafican que tiene el conjunto de bits del acuse de recibo (ACK).

Identifique los protocolos requeridos

El desarrollo de esta lista de protocolos requeridos puede ser una tarea desalentadora, pero hay varias técnicas que se pueden utilizar, según las necesidades, para ayudar a identificar el tráfico requerido.

- **Revise su política de seguridad / política de servicios**Su política de sitio local debería proporcionar una línea de base de los servicios permitidos y denegados.
- **Revise/audite su configuración de escudo de protección.**La configuración de escudo de protección actual debe contener las declaraciones explícitas del **permiso** para los servicios permitidos. En muchos casos, usted puede traducir esta configuración al formato ACL y utilizarla para crear el bulto de las entradas ACL.**Nota:** Generalmente, los firewalls de estado no poseen reglas explícitas para el tráfico de retorno a conexiones autorizadas. Debido a que las ACL de los routers no poseen estado, el tráfico de retorno debe ser permitido de manera explícita.
- **Revisión/auditoría de sus aplicaciones.**Las aplicaciones recibidas en el DMZ y ésas usadas internamente pueden ayudar a determinar los requisitos de filtración. Revise los requerimientos de la aplicación para proporcionar los detalles esenciales sobre el diseño de filtración.
- **Use una ACL de clasificación.**Una clasificación ACL se compone de las declaraciones del **permiso** para los diversos protocolos que se podrían destinar a la red interna. (Véase el Apéndice A para una lista de protocolos y de aplicaciones de uso general.) Utilice el **comando show access-list** de visualizar una cuenta de los golpes de la Entrada de control de acceso (ACE) para identificar los protocolos requeridos. Investigue y entienda cualquier resultado sospechoso o asombrosamente antes de que usted cree las declaraciones explícitas del **permiso** para los protocolos inesperados.
- **Utilice la característica conmutación Netflow.**El Netflow es una función de Switching que, si está habilitada, proporciona la información de flujo detallada. Si el Netflow se habilita en sus

routeres de borde, el **comando show ip cache flow** da una lista de protocolos registrados por el Netflow. El Netflow no puede identificar todos los protocolos, así que esta técnica se debe utilizar conjuntamente con otras.

Identifique el tráfico no válido

Además de la protección directa, el transitar ACL debe también proporcionar una primera línea de defensa contra los tipos determinados de tráfico no válido en el Internet.

- Niegue el espacio del RFC 1918.
- Niegue los paquetes con una dirección de origen que se caiga bajo espacio de la dirección del especial-uso, según lo definido en el RFC 3330.
- Aplique los filtros del anti-spoof, de acuerdo con el RFC 2827; su espacio de la dirección debe nunca ser la fuente de paquetes fuera de su sistema.

Otros tipos de tráfico a considerar incluyen:

- **Protocolos externos y IP Addresses que necesitan comunicar con el router de borde**ICMP de los IP Addresses del proveedor de servicioProtocolos de ruteoIPSec VPN, si utilizan a un router de borde como la terminación
- **Tráfico de retorno explícitamente permitido para las conexiones internas a Internet**Tipos específicos de Protocolo de mensaje de control de Internet (ICMP).Contestaciones salientes de la interrogación del Domain Name System (DNS)TCP establecidoTráfico de retorno del User Datagram Protocol (UDP)Conexiones de datos FTPConexiones de datos TFTPConexiones multimedia
- **Tráfico externamente originado explícitamente permitido destinado a las direcciones internas protegidas**Tráfico VPNInternet Security Association and Key Management Protocol (ISAKMP)Traversal del Network Address Translation (NAT)Encapsulación propietariaEncapsulating Security Payload (ESP)Encabezado de autenticaciónHTTP a los servidores WebSecure Socket Layer (SSL) a los servidores WebFTP a los servidores FTPConexiones de datos FTP entrantesConexiones de datos del pasivo FTP entrante (**pasv**)Protocolo Simple Mail Transfer (SMTP)Otras aplicaciones y servidoresInterrogaciones entrantes DNSTransferencias entrantes de la zona de DNS

Aplique el ACL

La ACL recientemente construida debería aplicarse al tráfico entrante en todas las interfaces orientadas a Internet de los routers de borde. En el ejemplo ilustrado en la sección de configuración típica, el ACL isapplied adentro en las interfaces de los Revestimientos del Internet en el IR1 y el IR2.

Vea las secciones en las Pautas para la instrumentación y el ejemplo de despliegue para más detalles.

Ejemplo de ACL

Esta lista de acceso proporciona un simple con todo el ejemplo realista de las entradas típicas requeridas en un transitar ACL. Es necesario personalizar esta ACL básica con los detalles de configuración locales específicos del sitio.

```
!--- Add anti-spoofing entries. !--- Deny special-use address sources. !--- Refer to RFC 3330
for additional special use addresses.

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
access-list 110 deny ip host 255.255.255.255 any
!--- The deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny ip host 0.0.0.0 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 !---
Permit Border Gateway Protocol (BGP) to the edge router. access-list 110 permit tcp host
bgp_peer gt 1023 host router_ip eq bgp access-list 110 permit tcp host bgp_peer eq bgp host
router_ip gt 1023 !--- Deny your space as source (as noted in RFC 2827). access-list 110 deny ip
your Internet-routable subnet any !--- Explicitly permit return traffic. !--- Allow specific
ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq 53 host primary DNS
server gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-list 110
permit udp any eq 53 host primary DNS server eq 53 !--- Permit legitimate business traffic.
access-list 110 permit tcp any Internet-routable subnet established access-list 110 permit udp
any range 1 1023 Internet-routable subnet gt 1023 !--- Allow ftp data connections. access-list
110 permit tcp any eq 20 Internet-routable subnet gt 1023 !--- Allow tftp data and multimedia
connections. access-list 110 permit udp any gt 1023 Internet-routable subnet gt 1023 !---
Explicitly permit externally sourced traffic. !--- These are incoming DNS queries.

access-list 110 permit udp any gt 1023 host <primary DNS server> eq 53
 !-- These are zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
secondary DNS server gt 1023 host primary DNS server eq 53 !--- Permit older DNS zone transfers.
access-list 110 permit tcp host secondary DNS server eq 53 host primary DNS server eq 53 !---
Deny all other DNS traffic. access-list 110 deny udp any any eq 53 access-list 110 deny tcp any
any eq 53 !--- Allow IPSec VPN traffic. access-list 110 permit udp any host IPSec headend device
eq 500 access-list 110 permit udp any host IPSec headend device eq 4500 access-list 110 permit
50 any host IPSec headend device access-list 110 permit 51 any host IPSec headend device access-
list 110 deny ip any host IPSec headend device !--- These are Internet-sourced connections to !-
-- publicly accessible servers. access-list 110 permit tcp any host public web server eq 80
access-list 110 permit tcp any host public web server eq 443 access-list 110 permit tcp any host
public FTP server eq 21 !--- Data connections to the FTP server are allowed !--- by the permit
established ACE. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host public FTP server gt 1023 access-list 110 permit tcp
any host public SMTP server eq 25 !--- Explicitly deny all other traffic.

access-list 101 deny ip any any
```

Nota: Tenga por favor estas sugerencias presente cuando usted aplica el transitar ACL.

- La palabra clave del **registro** se puede utilizar para proporcionar el detalle adicional sobre la fuente y los destinos para un protocolo dado. Aunque esta palabra clave proporcione el conocimiento valioso en los detalles de los golpes ACL, los golpes excesivos a una entrada ACL que utiliza la utilización de la CPU del aumento de la palabra clave del **registro**. El impacto del rendimiento asociado con el registro varía de acuerdo a la plataforma.
- Los mensajes inalcanzables de ICMP se generan para los paquetes que administrativo son negados por un ACL. Esto podría afectar el rendimiento del router y del link. Considere el uso

del **comando no ip unreachables** para inhabilitar los inalcanzables IP en la interfaz donde se despliega el transitar (borde) ACL.
- Este ACL se puede desplegar inicialmente con todas las declaraciones del **permiso** para asegurarse de que el tráfico legítimo del negocio no está negado. Una vez que se ha identificado y justificado el tráfico comercial legítimo, se pueden configurar los elementos de denegación específicos.

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. Los fragmentos noninitial que hacen juego las declaraciones de la capa 3 (protocolo, dirección de origen, y dirección destino) — con independencia de la información de la capa 4 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 noninitial con más granularity.

La filtración de los fragmentos agrega una capa adicional de protección contra un ataque de Negación de servicio (DoS) que utilice solamente los fragmentos noninitial (por ejemplo FO > 0). El uso de un **enunciado de negación** para los fragmentos noninitial al principio del ACL niega todos los fragmentos noninitial de acceder al router. En raras circunstancias, una sesión válida puede requerir fragmentación y, en consecuencia, ser filtrada si existe una sentencia de fragmento denegado en ACL. Las condiciones que pudieron llevar a la fragmentación incluyen el uso de los Certificados digitales para la autenticación ISAKMP y el uso del Traversal del IPSec NAT.

Por ejemplo, considere el ACL parcial mostrado aquí.

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

Agregar estas entradas al principio de un ACL niega cualquier acceso noninitial del fragmento a la red, 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 fragmento de ACL anterior también facilita la clasificación del ataque desde cada protocolo — UDP, TCP, y ICMP — los incrementos separa los contadores en el ACL.

Puesto que muchos ataques confían en la inundación con los paquetes fragmentados, la filtración de los fragmentos entrantes a la red interna proporciona una medida agregada de protección y las ayudas se aseguran de que un ataque no pueda inyectar los fragmentos simplemente correspondiendo con las reglas de la capa 3 en el transitar ACL.

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

Evaluación de riesgo

Cuando usted despliega la protección ACL del tráfico de tránsito, considere dos áreas claves del

riesgo.

- Asegúrese de que el **permiso**/los **enunciados de negación** apropiados exista. Para que el ACL sea eficaz, usted debe permitir todos los protocolos requeridos.
- El rendimiento de las ACL varía de la plataforma a la plataforma. Antes de que usted despliegue los ACL, revise las características del rendimiento de su hardware.

Cisco recomienda que usted prueba este diseño en el laboratorio antes del despliegue.

Apéndices

Protocolos y aplicaciones de uso general

Nombres de puertos TCP

Esta lista de nombres de puerto TCP se puede utilizar en vez de los números del puerto cuando usted configura el ACL en el Cisco IOS ® Software. Refiera al RFC del assigned number actual para encontrar una referencia a estos protocolos. ¿Los números del puerto que corresponden a estos protocolos pueden también ser encontrados por mientras que usted configura el ACL ingresando a**?** en lugar de un número del puerto.

bgp	kshell
chargen	login
cmd	lpd
durante el día	NNTP
Descartar	pim
domain	pop2
eco	pop3
exec	smtp
finger	sunrpc
FTP	syslog
datos ftp	tacacstalk
gopher	telnet
nombre del host	hora
ident	uucp
irc	WHOIS
klogin	WWW

Nombres de puertos UDP

Esta lista de nombres del puerto UDP se puede utilizar en vez de los números del puerto cuando usted configura el ACL en Cisco IOS Software. Refiera al RFC del assigned number actual para encontrar una referencia a estos protocolos. ¿Los números del puerto que corresponden a estos protocolos pueden también ser encontrados por mientras que usted configura el ACL ingresando a**?** en lugar de un número del puerto.

biff	ntp

Bootpc.	pim-auto-rp
bootps	rip
Descartar	snmp
dnsix	snmptrap
domain	sunrpc
eco	syslog
isakmp	tacacs
mobile-ip	charla
nombre del servidor	tftp
netbios-dgm	hora
netbios-ns	who
NetBios-SS	xdmcp

Pautas para la instrumentación

Cisco recomienda las prácticas conservadoras del despliegue. Usted debe tener un conocimiento de los protocolos requeridos para desplegar con éxito transita los ACL. Estas guías de consulta describen mismo un método conservador para el despliegue de la protección ACL que utilizan el acercamiento iterativo.

1. **Identifique los protocolos usados en la red con una clasificación ACL.**Despliegue un ACL que permita todos los protocolos conocidos que se utilizan en la red. Esta detección, o la clasificación, ACL debe tener una dirección de origen de **ningunos** y un destino de una dirección IP o de la subred entera del IP enrutable de Internet. Configure una entrada más reciente que permita que el **IP cualquier cualquier** orden del **login** ayude a identificar los protocolos adicionales que usted necesita permitir.El objetivo es determinar todos los protocolos requeridos que sean funcionando en la red. Utilice la registración para el análisis para determinar 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. Utilice la palabra clave del **registro** por los períodos cortos y solamente cuando es necesario para ayudar a clasificar el tráfico.Observe por favor que la red está a riesgo de ataque mientras que un ACL que consiste en todas las declaraciones del **permiso** existe. Realice el proceso de la clasificación lo más rápidamente posible para poder poner los controles de acceso apropiados en el lugar.
2. **Revise los paquetes identificados y comience a filtrar el acceso a la red interna.**Una vez identificados y revisados los paquetes filtrados por ACL en el paso 1, actualice la clasificación ACL para que contabilice los nuevos protocolos y direcciones IP identificadas. Agregue las entradas ACL para contra spoofing. Como sea necesario, el específico substituto **niega las** entradas para enunciados de permiso en la clasificación ACL. Usted puede utilizar el **comando show access-list** de monitorear el específico **niega las** entradas puede ser monitoreado para la cuenta del golpe. Proporciona información sobre los intentos de acceso de red prohibidos sin tener que habilitar el inicio de sesión en entradas ACL. La última línea de la ACL debe ser deny ip any any. De nuevo, la cuenta del golpe contra esta última entrada puede proporcionar la información sobre los intentos de acceso prohibidos.
3. **Monitoree y ponga al día el ACL.**Monitoree el ACL completado para asegurarse de que los

protocolos requeridos nuevamente introducidos están agregados en una manera controlada. Si usted monitorea el ACL, también proporciona la información sobre las tentativas prohibidas del acceso a la red que podrían proporcionar la información sobre los ataques inminentes.

Ejemplo de despliegue

Este ejemplo muestra un transitar ACL que proteja una red basada en esta dirección.

- La dirección IP del router del ISP es 10.1.1.1.La dirección IP de los Revestimientos del Internet del router de borde es 10.1.1.2.La subred con capacidad de ruteo de Internet es 192.168.201.0 255.255.255.0.La cabecera de VPN es 192.168.201.100.El servidor Web es 192.168.201.101.El servidor FTP es 192.168.201.102.El servidor SMTP es 192.168.201.103.El servidor DNS principal es 192.168.201.104.El servidor DNS secundario es 172.16.201.50.

La protección ACL del transitar fue desarrollada sobre la base de esta información. El ACL permite el eBGP que mira al router del ISP, proporciona los filtros del anti-spoof, permite el tráfico de retorno específico, permite el tráfico entrante específico, y niega explícitamente el resto del tráfico.

```
no access-list 110
!--- Phase 1 – Add anti-spoofing entries. !--- Deny special-use address sources. !--- See RFC
3330 for additional special-use addresses.

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
access-list 110 deny   ip host 255.255.255.255 any
!--- This deny statement should not be configured !--- on Dynamic Host Configuration Protocol
(DHCP) relays.

access-list 110 deny   ip host 0.0.0.0 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 !---
Permit BGP to the edge router. access-list 110 permit tcp host 10.1.1.1 gt 1023 host 10.1.1.2 eq
bgp access-list 110 permit tcp host 10.1.1.1 eq bgp host 10.1.1.2 gt 1023 !--- Deny your space
as source (as noted in RFC 2827). access-list 110 deny ip 192.168.201.0 0.0.0.255 any !--- Phase
2 – Explicitly permit return traffic. !--- Allow specific ICMP types.

access-list 110 permit icmp any any echo-reply
access-list 110 permit icmp any any unreachable
access-list 110 permit icmp any any time-exceeded
access-list 110 deny   icmp any any
!--- These are outgoing DNS queries. access-list 110 permit udp any eq domain host
192.168.201.104 gt 1023 !--- Permit older DNS queries and replies to primary DNS server. access-
list 110 permit udp any eq domain host 192.168.201.104 eq domain !--- Permit legitimate business
traffic. access-list 110 permit tcp any 192.168.201.0 0.0.0.255 established access-list 110
permit udp any range 1 1023 192.168.201.0 0.0.0.255 gt 1023 !--- Allow FTP data connections.
access-list 110 permit tcp any eq ftp-data 192.168.201.0 0.0.0.255 gt 1023 !--- Allow TFTP data
and multimedia connections. access-list 110 permit udp any gt 1023 192.168.201.0 0.0.0.255 gt
1023 !--- Phase 3 – Explicitly permit externally sourced traffic. !--- These are incoming DNS
queries.

access-list 110 permit udp any gt 1023 host 192.168.201.104 eq domain
!--- Zone transfer DNS queries to primary DNS server. access-list 110 permit tcp host
172.16.201.50 gt 1023 host 192.168.201.104 eq domain !--- Permit older DNS zone transfers.
```

```
access-list 110 permit tcp host 172.16.201.50 eq domain host 192.168.201.104 eq domain !--- Deny all other DNS traffic. access-list 110 deny udp any any eq domain access-list 110 deny tcp any any eq domain !--- Allow IPSec VPN traffic. access-list 110 permit udp any host 192.168.201.100 eq isakmp access-list 110 permit udp any host 192.168.201.100 eq non500-isakmp access-list 110 permit esp any host 192.168.201.100 access-list 110 permit ahp any host 192.168.201.100 access-list 110 deny ip any host 192.168.201.100 !--- These are Internet-sourced connections to !--- publicly accessible servers. access-list 110 permit tcp any host 192.168.201.101 eq www access-list 110 permit tcp any host 192.168.201.101 eq 443 access-list 110 permit tcp any host 192.168.201.102 eq ftp !--- Data connections to the FTP server are allowed !--- by the permit established ACE in Phase 3. !--- Allow PASV data connections to the FTP server.

access-list 110 permit tcp any gt 1023 host 192.168.201.102 gt 1023
access-list 110 permit tcp any host 192.168.201.103 eq smtp

!--- Phase 4 – Add explicit deny statement.

access-list 110 deny   ip any any

Edge-router(config)#interface serial 2/0
Edge-router(config-if)#ip access-group 110 in
```

Información Relacionada

- Páginas de Soporte de Listas de Acceso
- Referencia de comandos del Cisco IOS Switching Services, Release12.2 - Comandos: tarifa-límite de la lista de acceso a través del cef del IP
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems