Configuración de la lista de control de acceso ASA para diversos escenarios

Contenido

Introducción

Este documento describe cómo configurar una lista de control de acceso (ACL) en el dispositivo de seguridad adaptable (ASA) para varios escenarios.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos de ASA.

Componentes Utilizados

La información de este documento se basa en la versión 8.3 y posteriores del software ASA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El ASA utiliza las ACL para determinar si el tráfico está permitido o denegado. De forma predeterminada, el tráfico que pasa de una interfaz de nivel de seguridad **inferior** a una interfaz de nivel de seguridad **superior** es denegado, mientras que el tráfico de una interfaz de nivel de seguridad **superior** a una interfaz de nivel de seguridad **inferior** es permitido. También es posible anular este comportamiento con una ACL.

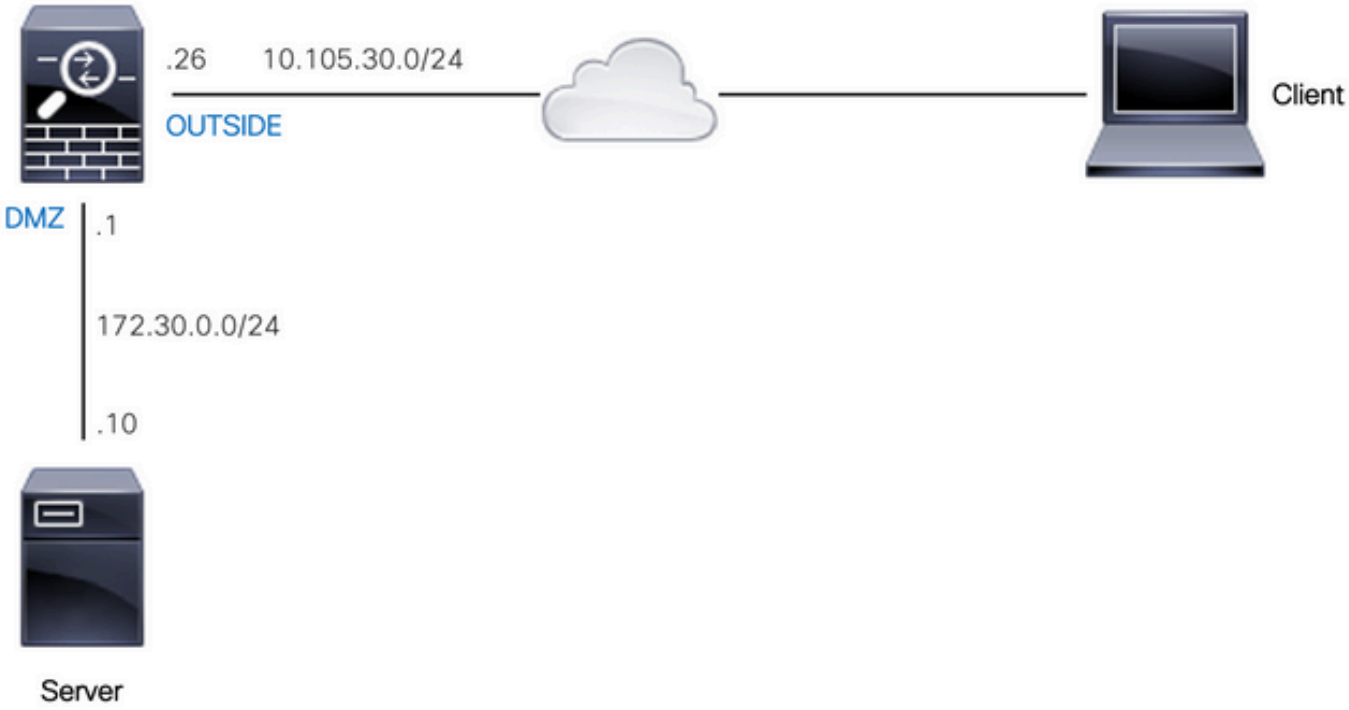
En presencia de reglas NAT, en versiones anteriores de ASA (8.2 y anteriores), ASA verifica la ACL antes de anular la traducción del paquete en función de la regla NAT que coincidió. En la versión 8.3 y posteriores, ASA cancela la traducción del paquete antes de verificar las ACL. Esto significa que para una versión de ASA 8.3 y posteriores, el tráfico se permite o se niega en función de la dirección IP real del host en lugar de la dirección IP traducida. Las ACL se componen de una o más entradas de control de acceso (ACE).

Configurar

Escenario 1. Configuración de un ACE para permitir el acceso a un servidor web ubicado detrás de la DMZ

El cliente de Internet, situado detrás de la interfaz externa, desea acceder a un servidor web alojado detrás de la interfaz DMZ que escucha en los puertos TCP 80 y 443.

Diagrama de la red



La dirección IP real del servidor Web es 172.30.0.10. Se configura una regla NAT uno a uno estática para permitir que los usuarios de Internet accedan al servidor web con una dirección IP traducida 10.105.130.27. El ASA realiza un proxy-arp para 10.105.130.27 en la interfaz 'externa' de manera predeterminada cuando una regla NAT estática se configura con una dirección IP traducida que cae en la misma subred que la dirección IP de la interfaz 'externa' 10.105.130.26:

```
object network web-server
nat (dmz,outside) static 10.105.130.27
```

Configure esta ACE para permitir que cualquier dirección IP de origen en Internet se conecte al servidor Web sólo en los puertos TCP 80 y 443. Asigne la ACL a la interfaz exterior en la dirección entrante:

```
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq www
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
access-group OUT-IN in interface outside
```

Verificación

Ejecute un comando packet-tracer con estos campos. Interfaz de ingreso en la que se debe rastrear el paquete: externo

Protocolo: TCP

Dirección IP de origen: cualquier dirección IP de Internet

Puerto IP de origen: cualquier puerto efímero

Dirección IP de destino: dirección IP traducida del servidor web (10.105.130.27)

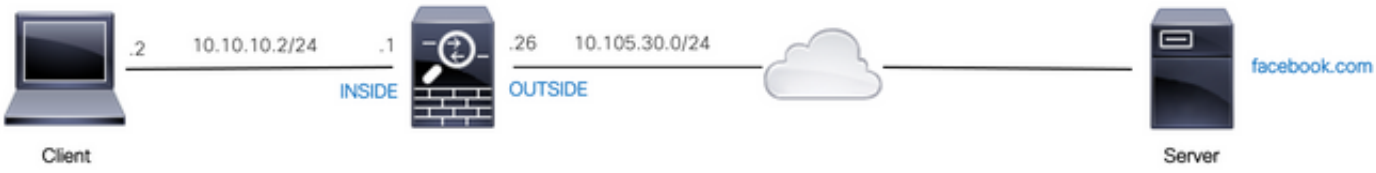
Puerto de destino: 80 o 443

```
ciscoasa# packet-tracer input outside tcp 10.0.50.50 1234 10.105.130.27 443

!--- NAT untranslate from 10.105.130.27/443 to 172.30.0.10/443


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network web-server
nat (dmz,outside) static 10.105.130.27
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.105.130.27/443 to 172.30.0.10/443

!--- The configured ACL is permitting this packet to 172.30.0.10 on TCP port 443


Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUT-IN in interface outside
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
Additional Information:

!--- Final result shows allow from the outside interface to the dmz interface

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Situación hipotética 2. Configurar un ACE para permitir el acceso a un servidor web con un FQDN

El cliente con la dirección IP 10.10.10.2 ubicada en la red de área local (LAN) puede acceder a facebook.com.

Diagrama de la red



Asegúrese de que el servidor DNS esté configurado correctamente en el ASA:

```
ciscoasa# show run dns
dns domain-lookup outside
dns server-group DefaultDNS
```

```
name-server 10.0.2.2
name-server 10.0.8.8
```

Configure este objeto de red, el objeto FQDN y la ACE para permitir que el cliente con la dirección IP 10.10.10.2 acceda a facebook.com.

```
object network obj-10.10.10.2
host 10.10.10.2

object network obj-facebook.com
fqdn facebook.com

access-list IN-OUT extended permit ip object obj-10.10.10.2 object obj-facebook.com
access-group IN-OUT in interface inside
```

Verificación

El resultado de **show dns** muestra la dirección IP resuelta para el FQDN facebook.com:

```
ciscoasa# show dns

Host Flags Age Type Address(es)
facebook.com (temp, OK) 0 IP 10.0.228.35
```

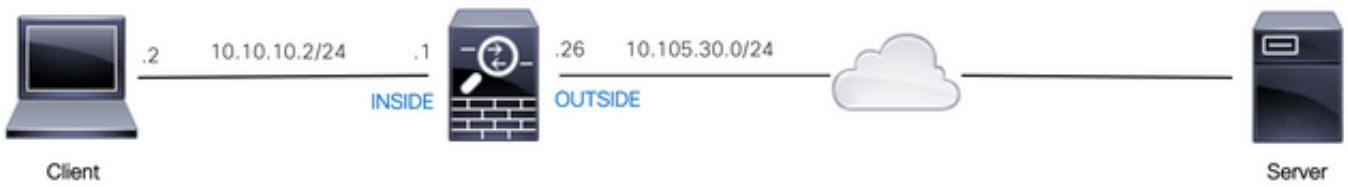
La lista de acceso muestra el objeto FQDN como **resuelto** y también muestra la dirección IP resuelta:

```
ciscoasa# show access-list IN-OUT
access-list IN-OUT; 2 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip object obj-10.10.10.2 object obj-facebook.com
(hitcnt=1) 0x22075b2a
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 fqdn facebook.com (resolved)
0xfea095d7
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 host 10.0.228.35 (facebook.com)
(hitcnt=1) 0x22075b2a
```

Situación hipotética 3. Configuración de un As para permitir el acceso a un sitio web solo durante un período de tiempo específico en un día

El cliente ubicado en la LAN tiene permiso para acceder a un sitio web con dirección IP 10.0.20.20 diariamente de 12 PM a 2 PM IST solamente.

Diagrama de la red



Asegúrese de que la zona horaria esté configurada correctamente en el ASA:

```
ciscoasa# show run clock
clock timezone IST 5 30
```

Configure un objeto de rango de tiempo para la duración requerida:

```
time-range BREAK_TIME
periodic daily 12:00 to 14:00
```

Configure estos objetos de red y ACE para permitir que cualquier dirección IP de origen ubicada en la LAN acceda al sitio web solamente durante el período de tiempo mencionado en el objeto de rango de tiempo denominado **BREAK_TIME:**

```
object network obj-website
host 10.0.20.20


access-list IN-OUT extended permit ip any object obj-website time-range BREAK_TIME
access-group IN-OUT in interface inside
```

Verificación

El objeto de rango de tiempo está **activo** cuando el reloj en el ASA indica una hora que está dentro del objeto de rango de tiempo:

```
ciscoasa# show clock
12:03:41.987 IST Mon Oct 4 2021


ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (active)
periodic daily 12:00 to 14:00
used in: IP ACL entry


ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
```

El objeto de rango de tiempo así como la ACE están **inactivos** cuando el reloj en el ASA indica una hora que está fuera del objeto de rango de tiempo:

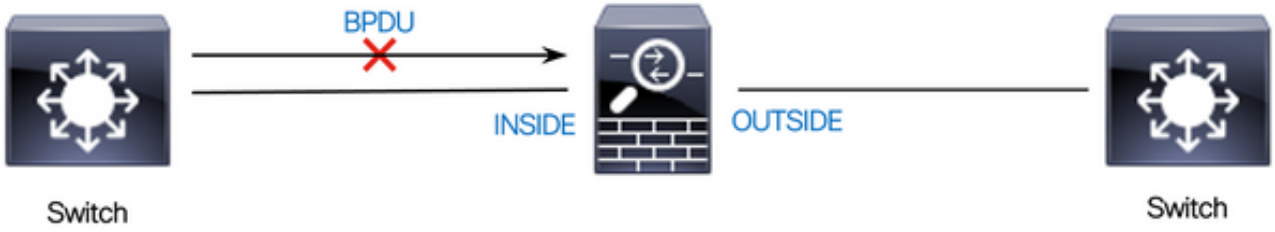
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (inactive)
periodic daily 12:00 to 14:00
used in: IP ACL entry


ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=0) (inactive) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
```

```
(hitcnt=0) (inactive) 0x5a66c8f9
```

Situación hipotética 4. Configuración de una Ace para Bloquear las Unidades de Datos del Protocolo de Bridge (Bpdu) a través de un ASA en Modo Transparente

Para evitar bucles con el protocolo de árbol de extensión (STP), las BPDU pasan a través del ASA en modo transparente de forma predeterminada. Para bloquear las BPDU, debe configurar una regla EtherType para denegarlas.

Diagrama de la red



Configure la ACL EtherType para bloquear las BPDU de modo que no pasen a través de la interfaz 'interna' del ASA en la dirección entrante, como se muestra aquí:

```
access-list block-bpdu ethertype deny dsap bpdu
access-list block-bpdu ethertype permit any
access-group block-bpdu in interface inside
```

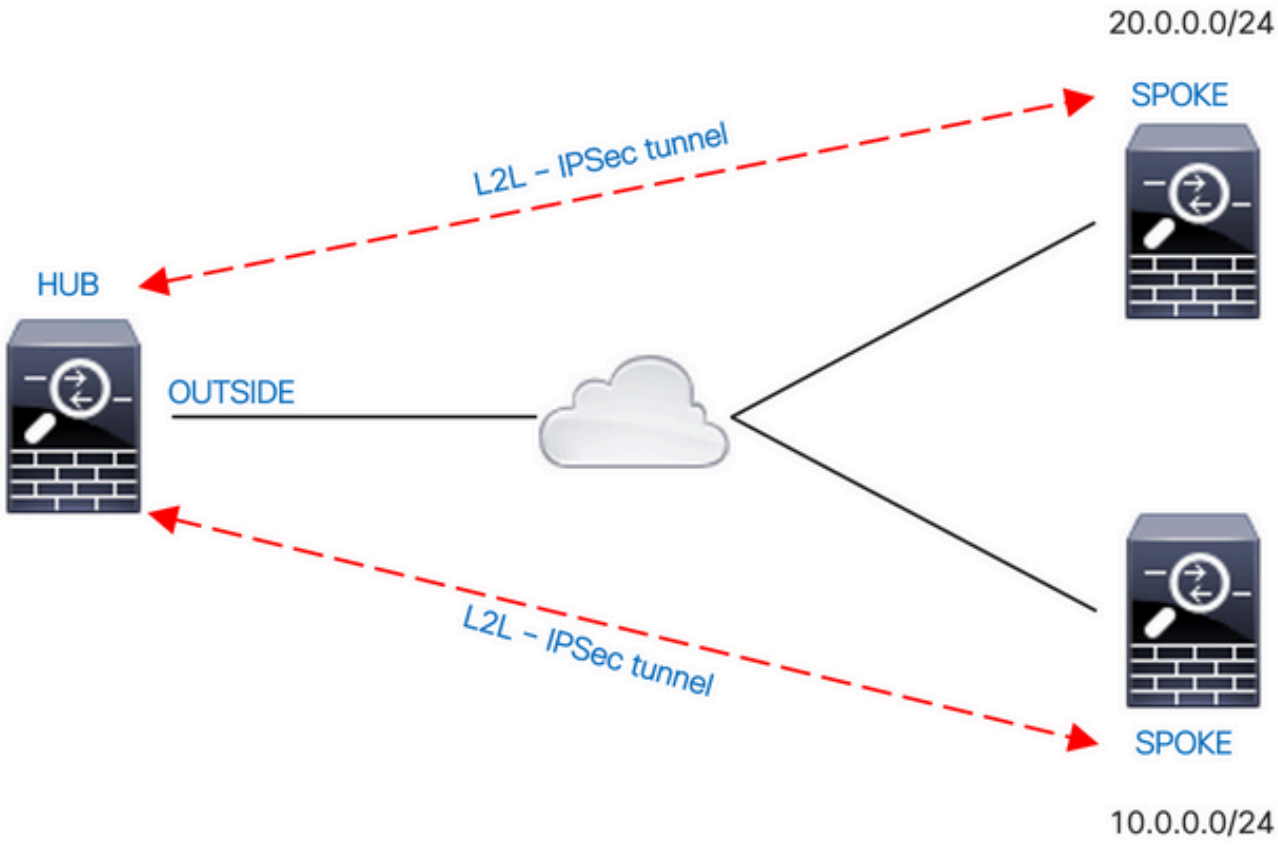
Verificación

Verifique el conteo de llamadas en la lista de acceso para verificar que las BPDU estén bloqueadas por el ASA:

```
ciscoasa# show access-list block-bpdu
access-list block-bpdu; 2 elements
access-list block-bpdu ethertype deny dsap bpdu(hitcount=14)
access-list block-bpdu ethertype permit any (hitcount=48)
```

Situación hipotética 5. Permitir que el tráfico pase entre interfaces con el mismo nivel de seguridad

Diagrama de la red



De forma predeterminada, el tráfico que pasa entre interfaces del mismo nivel de seguridad se bloquea. Para permitir la comunicación entre interfaces con niveles de seguridad iguales, o para permitir que el tráfico entre y salga de la misma interfaz (hairpin/u-turn), utilice el comando **same-security-traffic** en el modo de configuración global.

Este comando muestra cómo permitir la comunicación entre diferentes interfaces que tienen el mismo nivel de seguridad:

```
same-security-traffic permit inter-interface
```

Este ejemplo muestra cómo permitir la comunicación dentro y fuera de la misma interfaz:

```
same-security-traffic permit intra-interface
```

Esta característica es útil para el tráfico VPN que ingrese una interfaz pero después se rutea fuera de esa misma interfaz. Por ejemplo, si tiene una red VPN hub-and-spoke donde este ASA es el hub y las redes VPN remotas son spokes, para que un spoke se comunique con otro spoke, el tráfico debe ir al ASA y luego salir nuevamente al otro spoke.

Verificación

Sin el comando **same-security-traffic permit inter-interface**, la salida de packet-tracer indica que el tráfico que pasa entre diferentes interfaces del mismo nivel de seguridad está bloqueado debido a una **regla implícita** como se muestra aquí:

```
!--- The interfaces named 'test' and 'outside' have the same security level of 0

ciscoasa# show nameif
```

```
Interface Name Security
GigabitEthernet0/0 inside 100
GigabitEthernet0/1 dmz 50
GigabitEthernet0/2 test 0
GigabitEthernet0/5 outside 0
Management0/0 mgmt 0

!--- Traffic between different interfaces of same security level is blocked by an implicit rule

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a2ff90, priority=110, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=test, output_ifc=any

Result:
input-interface: test
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA


!--- After running the command 'same-security-traffic permit inter-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit inter-interface

!--- Traffic between different interfaces of same security level is allowed

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a352d0, priority=2, domain=permit, deny=false
hits=2, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=test, output_ifc=any

Result:
input-interface: test
input-status: up
```

```
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Sin el comando **same-security-traffic permit intra-interface**, la salida de packet-tracer indica que el tráfico que entra y sale de la misma interfaz está bloqueado debido a una **regla implícita** como se muestra aquí:

```
!--- Traffic in and out of the same interface is blocked by an implicit rule

ciscoasa# packet-tracer input outside tcp 10.0.0.10 1234 10.1.0.10 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a32f30, priority=111, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=outside, output_ifc=outside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA

!--- After running the command 'same-security-traffic permit intra-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit intra-interface


!--- Traffic in and out of the same interface is allowed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f99609291c0, priority=3, domain=permit, deny=false
hits=1, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=outside, output_ifc=outside
```

```
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Situación hipotética 6. Configuración de un ACE para controlar el tráfico directo

La palabra clave **control-plane** especifica si la ACL se utiliza para controlar el tráfico a la interfaz. Las reglas de control de acceso para el tráfico de administración directa (definidas por comandos como **http**, **ssh** o **telnet**) tienen mayor prioridad que una regla de acceso de administración aplicada con la opción **plano de control**. Por lo tanto, se debe permitir que dicho tráfico de administración permitido entre incluso si lo niega explícitamente la ACL de fábrica.

A diferencia de las reglas de acceso normales, no hay una denegación implícita al final de un conjunto de reglas de administración para una interfaz. En su lugar, cualquier conexión que no coincida con una regla de acceso a la administración se evalúa mediante reglas de control de acceso normales. Alternativamente, puede utilizar reglas ICMP para controlar el tráfico ICMP al dispositivo.

Diagrama de la red

Una ACL se configura con la palabra clave **control-plane** para bloquear el tráfico "to-the-box" originado en la dirección IP 10.65.63.155 y destinado a la dirección IP de la interfaz 'externa' del ASA.

```
access-list control-plane-test extended deny ip host 10.65.63.155 any
access-group control-plane-test in interface outside control-plane
```

Verificación

Verifique el conteo de visitas en la lista de acceso para verificar que el tráfico está bloqueado por la ACL:

```
ciscoasa# show access-list control-plane-test
access-list control-plane-test; 1 elements; name hash: 0x6ff5e700
access-list control-plane-test line 1 extended deny ip host 10.65.63.155 any (hitcnt=4)
0xedad4c6f
```

Los mensajes de Syslog indican que el tráfico se descarta en la interfaz de 'identidad':

```
Dec 27 2021 13:19:44: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:45: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:46: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:47: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
```

Registro

La palabra clave **log** establece las opciones de registro cuando una ACE coincide con un paquete para el acceso a la red (una ACL aplicada con el comando **access-group**). Si ingresa la palabra clave **log** sin ningún argumento, habilite el mensaje de registro del sistema 106100 en el nivel predeterminado (6) y para el intervalo predeterminado (300 segundos). Si no introduce la palabra clave log, se genera el mensaje de registro del sistema 106023 predeterminado para los paquetes denegados. Las opciones de registro son:

- nivel: un nivel de gravedad entre 0 y 7. El valor predeterminado es 6 (informativo). Si cambia este nivel para una ACE activa, el nuevo nivel se aplica a las nuevas conexiones; las conexiones existentes se siguen registrando en el nivel anterior.
- **interval** secs: intervalo de tiempo en segundos entre mensajes de syslog, de 1 a 600. El valor predeterminado es 300. Este valor también se utiliza como valor de tiempo de espera para eliminar un flujo inactivo de la memoria caché utilizado para recopilar estadísticas de caídas.
- **disable**: deshabilita todos los registros ACE.
- **default** — habilita el registro en el mensaje 106023. Esta configuración equivale a no incluir la opción de registro.

Mensaje de Syslog 106023:

```
Message:
%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user
|FQDN_string ], sg_info )] dst interface_name :dest_address /dest_port [([idfw_user |FQDN_string
], sg_info )] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]
```

Explicación:

La ACL denegó un paquete IP real. Este mensaje aparece incluso si no tiene la opción de registro habilitada para una ACL. La dirección IP es la dirección IP real en lugar de los valores que se muestran a través de NAT. Tanto la información de identidad del usuario como la información de FQDN se proporcionan para las direcciones IP si se encuentra una que coincida. El ASA de Secure Firewall registra información de identidad (dominio\usuario) o FQDN (si el nombre de usuario no está disponible). Si la información de identidad o FQDN está disponible, Secure Firewall ASA registra esta información para el origen y el destino.

Ejemplo:

```
Dec 27 2021 14:58:25: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
Dec 27 2021 14:58:26: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
Dec 27 2021 14:58:27: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
```

Mensaje de Syslog 106100:

Message:

%ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} *protocol interface_name /source_address (source_port) (idfw_user , sg_info) interface_name /dest_address (dest_port) (idfw_user , sg_info)* hit-cnt *number* ({first hit | *number* -second interval}) hash codes

Explicación:

Se muestra la aparición inicial o el número total de apariciones durante un intervalo. Este mensaje proporciona más información que el mensaje 106023, que sólo registra los paquetes denegados y no incluye el conteo de aciertos ni un nivel configurable.

Cuando una línea de la lista de acceso tiene el argumento *log*, se espera que este ID de mensaje pueda ser disparado debido a que un paquete no sincronizado llega a Secure Firewall ASA y es evaluado por la lista de acceso. Por ejemplo, si se recibe un paquete ACK en Secure Firewall ASA (para el que no existe ninguna conexión TCP en la tabla de conexión), Secure Firewall ASA puede generar el mensaje 106100, que indica que se permitió el paquete; sin embargo, el paquete se descarta correctamente más adelante debido a que no hay ninguna conexión coincidente.

La lista describe los valores del mensaje:

- permitido | denegado | est-allowed: Estos valores especifican si la ACL permitió o denegó el paquete. Si el valor es est-allowed, el paquete fue negado por la ACL pero fue permitido para una sesión ya establecida (por ejemplo, un usuario interno es permitido acceder a Internet, y los paquetes que responderían que serían negados normalmente por la ACL son aceptados).
- protocol: TCP, UDP, ICMP o un número de protocolo IP.
- interface_name: el nombre de la interfaz para el origen o el destino del flujo registrado. Las interfaces VLAN son compatibles.
- source_address: la dirección IP de origen del flujo registrado. La dirección IP es la dirección IP real en lugar de los valores que se muestran a través de NAT.
- dest_address: la dirección IP de destino del flujo registrado. La dirección IP es la dirección IP real en lugar de los valores que se muestran a través de NAT.
- source_port: el puerto de origen del flujo registrado (TCP o UDP). Para ICMP, el número después del puerto de origen es el tipo de mensaje.
- idfw_user: el nombre de usuario de la identidad del usuario, con el nombre de dominio que se agrega al syslog existente cuando Secure Firewall ASA puede encontrar el nombre de usuario para la dirección IP.
- sg_info: la etiqueta de grupo de seguridad que se agrega al syslog cuando el ASA de Secure Firewall puede encontrar una etiqueta de grupo de seguridad para la dirección IP. El nombre del grupo de seguridad se muestra con la etiqueta del grupo de seguridad, si está disponible.
- dest_port: el puerto de destino del flujo registrado (TCP o UDP). Para ICMP, el número después del puerto de destino es el código de mensaje ICMP, que está disponible para algunos tipos de mensajes. Para el tipo 8, siempre es 0. Para obtener una lista de los tipos de mensajes ICMP, consulte la URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- número de hit-cnt: la cantidad de veces que esta entrada de ACL permitió o denegó este flujo en el intervalo de tiempo configurado. El valor es 1 cuando Secure Firewall ASA genera el primer mensaje para este flujo.

- primer resultado: el primer mensaje generado para este flujo.
- número - segundo intervalo: intervalo en el que se acumula el recuento de visitas. Establezca este intervalo con el comando **access-list** con la opción **interval**.
- códigos hash: siempre se imprimen dos para el grupo de objetos ACE y la ACE regular constituyente. Los valores se determinan en qué ACE el paquete golpea. Para mostrar estos códigos hash, ingrese el comando **show-access list**.

Ejemplo:

```
Dec 27 2021 15:09:58: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56261) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:15: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56266) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:55: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56270) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).