Prácticas recomendadas de ACL en un router serie RV34x

Objetivo

El objetivo de este artículo es describir las prácticas recomendadas para crear listas de control de acceso (ACL) con el router serie RV34x.

Dispositivos aplicables | Versión del firmware

- RV340 | 1.0.03.20 (descargar último)
- RV340W | 1.0.03.20 (descargar último)
- RV345 | 1.0.03.20 (descargar último)
- RV345P | 1.0.03.20 (descargar último)

Introducción

¿Desea más control sobre su red? ¿Desea realizar pasos adicionales para mantener la seguridad de su red? Si es así, es posible que una lista de control de acceso (ACL) sea exactamente lo que necesita.

Una ACL consta de una o más entradas de control de acceso (ACE) que definen colectivamente el perfil de tráfico de red. A continuación, las funciones de software de Cisco pueden hacer referencia a este perfil, como el filtrado de tráfico, la prioridad o la colocación en cola personalizada. Cada ACL incluye un elemento de acción (permit o deny) y un elemento de filtro basado en criterios como la dirección de origen, la dirección de destino, el protocolo y los parámetros específicos del protocolo.

Según los criterios que haya especificado, puede controlar que cierto tráfico entre y/o salga de una red. Cuando un router recibe un paquete, examina el paquete para determinar si reenvía o descarta el paquete según su lista de acceso.

La implementación de este nivel de seguridad se basa en diferentes casos prácticos, teniendo en cuenta las necesidades de seguridad y escenarios de red particulares.

Es importante tener en cuenta que el router puede hacer automáticamente una lista de acceso basada en las configuraciones del router. En este caso, puede ver listas de acceso que no puede borrar a menos que cambie las configuraciones del router.

Por qué utilizar las listas de acceso

- En la mayoría de los casos, utilizamos ACL para proporcionar un nivel básico de seguridad para acceder a nuestra red. Por ejemplo, si no configura las ACL, de forma predeterminada todos los paquetes que pasan a través del router podrían estar permitidos en todas las partes de nuestra red.

- Las ACL pueden permitir que un host, un intervalo de direcciones IP o redes y evitar que otro host, un intervalo de direcciones IP o redes accedan al mismo área (host o red).
- Mediante ACL, puede decidir qué tipos de tráfico reenvió o bloqueó en las interfaces del router. Por ejemplo, puede permitir el tráfico de protocolo de transferencia de archivos (SFTP) de Secure Shell (SSH) y, al mismo tiempo, bloquear todo el tráfico de protocolo de inicio de sesión (SIP).

Cuándo utilizar las listas de acceso

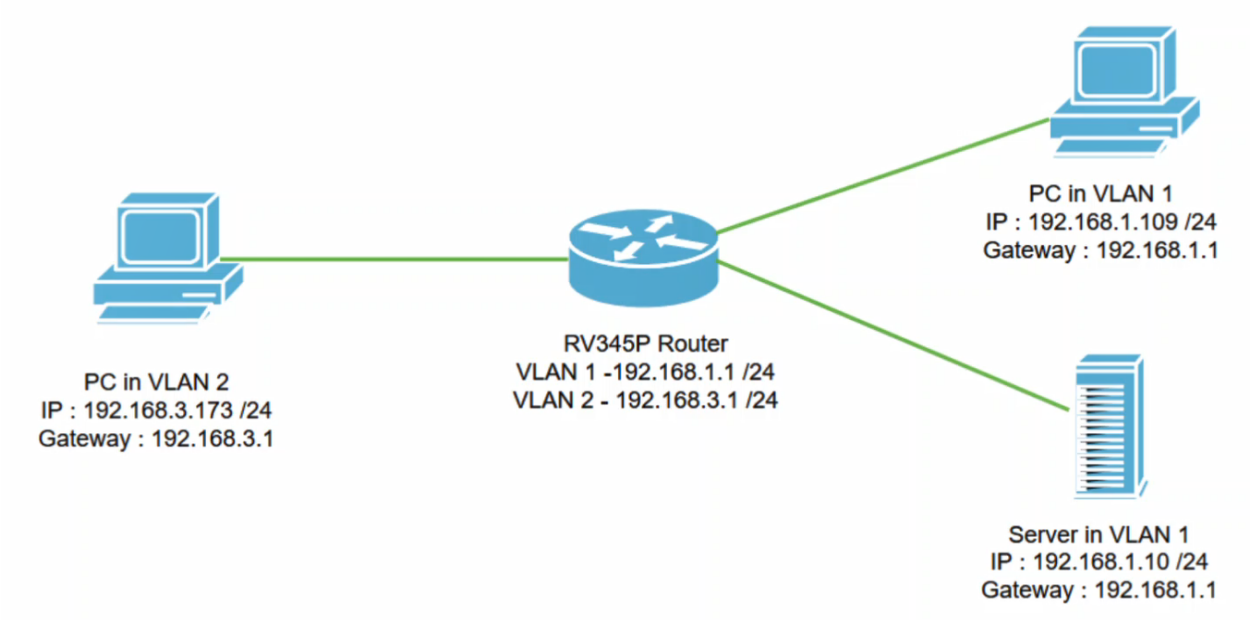
- Debe configurar las ACL en los routers situados entre nuestra red interna y una red externa como Internet.
- Puede utilizar las ACL para controlar el tráfico que entra o sale de una parte específica de nuestra red interna.
- Cuando necesita filtrar el tráfico entrante o saliente, o ambos en una interfaz.
- Debe definir las ACL por protocolo para controlar el tráfico.

Prácticas recomendadas para configurar la seguridad básica con listas de acceso

- Implemente ACL que permiten solamente los protocolos, puertos y direcciones IP que niegan todo lo demás.
- Bloquear los paquetes entrantes que afirman tener el mismo destino y la misma dirección de origen (ataque terrestre en el propio router).
- Active la función de registro en las ACL a un host interno (de confianza) de Syslog.
- Si utiliza el protocolo simple de administración de red (SNMP) en el router, debe configurar la ACL SNMP y la cadena de comunidad SNMP compleja.
- Permitir que sólo las direcciones internas ingresen al router desde las interfaces internas y permitir que sólo el tráfico destinado a las direcciones internas ingrese al router desde el exterior (interfaces externas).
- Bloquee la multidifusión si no se utiliza.
- Bloquear algunos tipos de mensajes de protocolo de mensajes de control de Internet (ICMP) (redirección, eco).
- Tenga siempre en cuenta el orden en el que ingresa las ACL. Por ejemplo, cuando el router decide si reenviar o bloquear un paquete, prueba el paquete con cada sentencia ACL en el orden en que se crearon las ACL.

Implementación de la lista de acceso en los routers Cisco RV34x Series

Topología de red de ejemplo



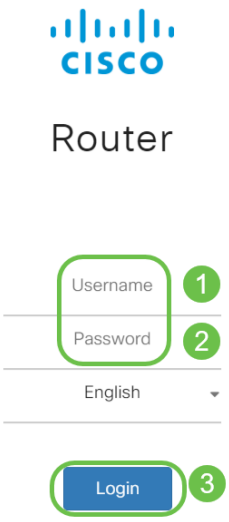
Situación de ejemplo

En este escenario, replicaremos este diagrama de red, donde tenemos un router RV345P y dos interfaces VLAN diferentes. Tenemos un PC en VLAN 1 y en VLAN2, y también tenemos un servidor en VLAN 1. El ruteo entre VLAN está habilitado, por lo que los usuarios de VLAN 1 y VLAN 2 pueden comunicarse entre sí. Ahora vamos a aplicar la regla de acceso para restringir la comunicación entre el usuario de VLAN 2 hacia este servidor en VLAN 1.

Configuración de ejemplo

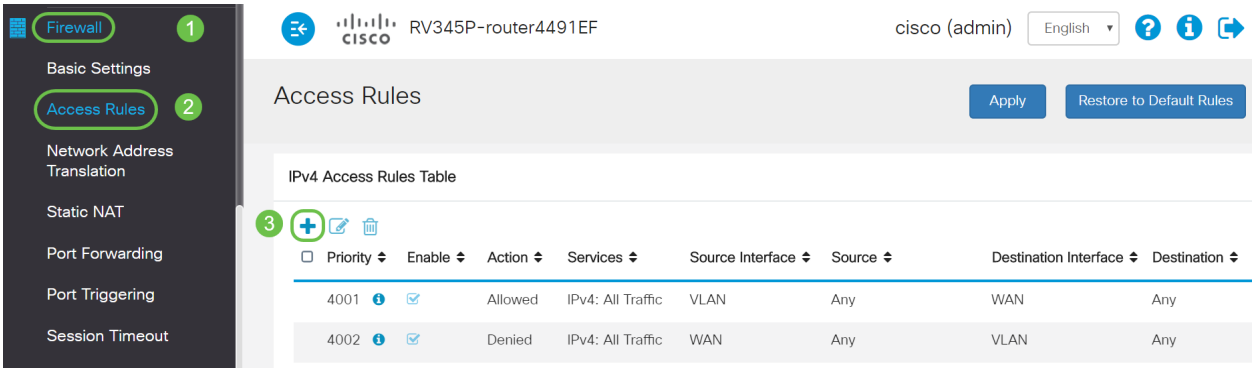
Paso 1

Inicie sesión en la interfaz de usuario web (IU) del router mediante las credenciales que ha configurado.



Paso 2

Para configurar la ACL, navegue hasta **Firewall > Access Rules** y haga clic en el **icono plus** para agregar una nueva regla.



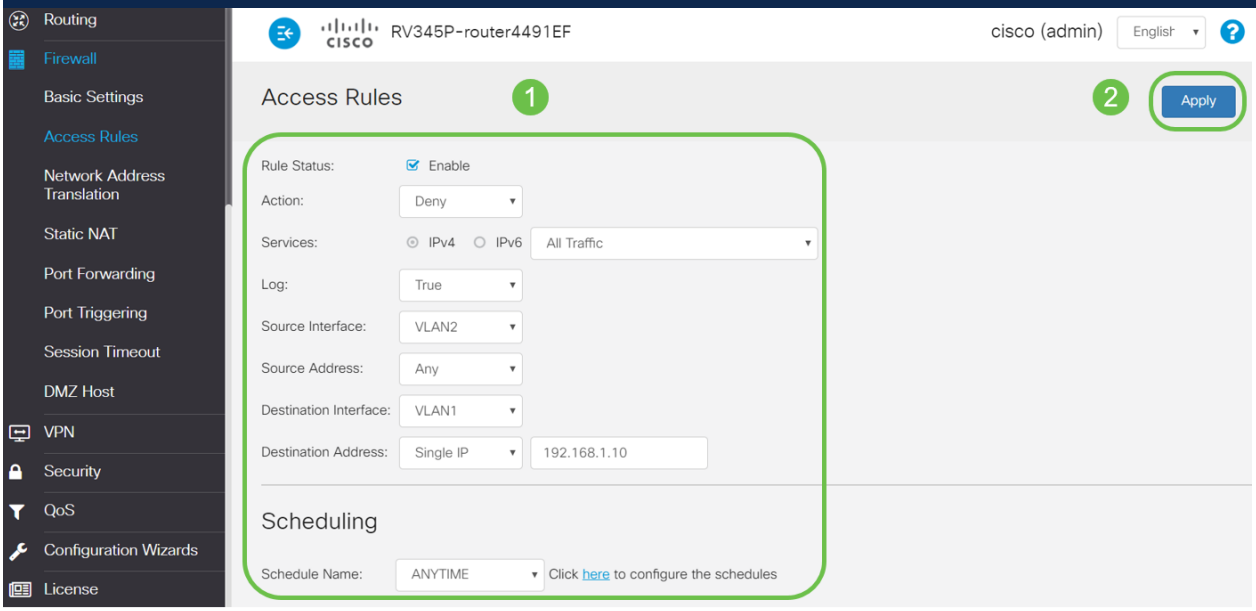
Paso 3

Configure los parámetros *de las reglas de acceso*. Aplicar ACL para restringir el servidor (IPv4: 192.168.1.10/24) de los usuarios de VLAN2. Para este escenario, los parámetros serán los siguientes:

- *Estado de la regla: Habilitar*
- *Acción: Denegar*
- *Servicios: Todo el tráfico*
- *Registro: Verdadero*
- *Interfaz de origen: VLAN2*
- *Dirección de la fuente: cualquiera*
- *Interfaz de destino: VLAN1*
- *dirección de destino: IP única 192.168.1.10*
- *Nombre de la programación: En cualquier momento*

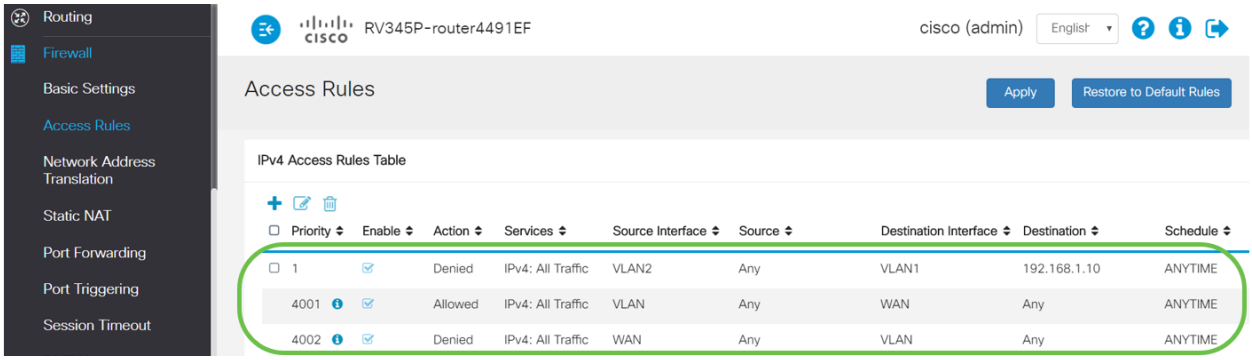
Haga clic en Apply (Aplicar).

En este ejemplo, negamos el acceso desde cualquier dispositivo desde VLAN2 al servidor y luego permitimos el acceso a los otros dispositivos en VLAN1. Sus necesidades pueden variar.



Paso 4

La lista *Reglas de acceso* mostrará lo siguiente:



Verificación

Para verificar el servicio, abra el símbolo del sistema. En las plataformas Windows, esto se puede lograr haciendo clic en el botón Windows y después escribiendo **cmd** en el cuadro de búsqueda inferior izquierda del equipo y seleccionando **símbolo del sistema** en el menú.

Ingrese los siguientes comandos:

- En PC (192.168.3.173) en VLAN2, haga ping en el servidor (IP: 192.168.1.10). Recibirá una notificación *de tiempo de espera agotado de la solicitud*, lo que significa que no se permite la comunicación.
- En PC (192.168.3.173) en VLAN2, haga ping en el otro PC (192.168.1.109) en VLAN1. Obtendrá una respuesta satisfactoria.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

Conclusión

Ha visto los pasos necesarios para configurar la regla de acceso en un Cisco RV34x Series Router. Ahora puede aplicarlo para crear una regla de acceso en su red que se ajuste a sus necesidades.