Resolución de problemas de listas de acceso a través de la red privada virtual en los routers VPN RV016, RV042, RV042G y RV082

Objetivos

Una lista de control de acceso (ACL) es una colección de condiciones de permiso y denegación. Una ACL especifica a qué usuarios o procesos del sistema se les concede acceso a recursos específicos. Una ACL puede bloquear cualquier intento injustificado de alcanzar recursos de red. El problema en esta situación puede surgir cuando tiene ACL configuradas en ambos routers pero uno de los routers no puede diferenciar entre las listas de tráfico permitido y denegado permitidas por la ACL. Zenmap, que es una herramienta de código abierto utilizada para verificar el tipo de filtros de paquetes/firewalls activos, se utiliza para probar la configuración.

En este artículo se explica cómo resolver problemas de las ACL permitidas que no funcionan en una VPN de gateway a gateway entre dos routers VPN.

Dispositivos aplicables

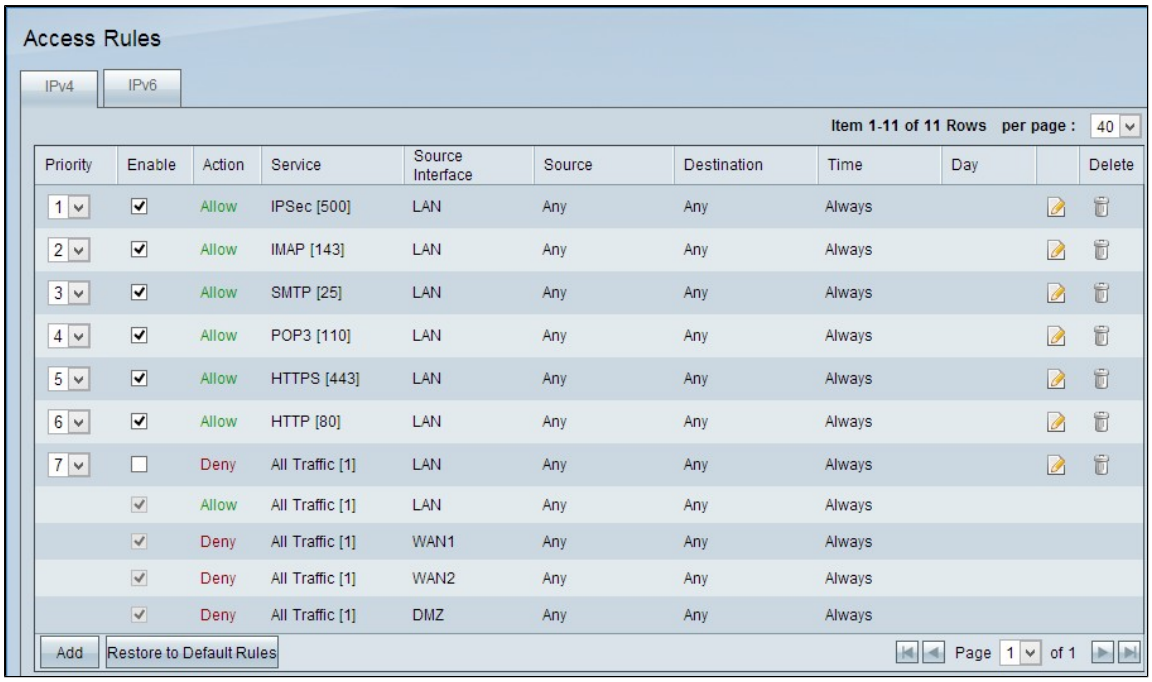
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Versión del software

â€¢v4.2.2.08

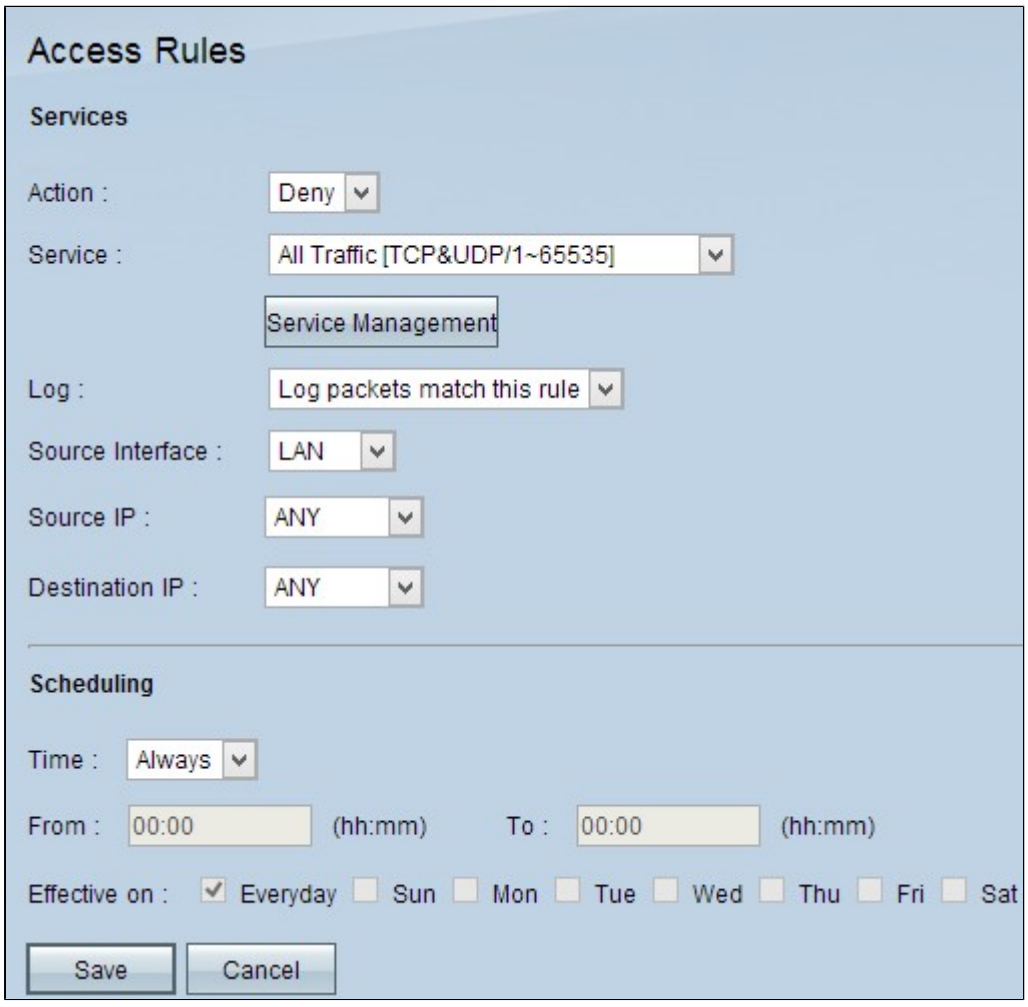
Configuración de ACL sobre VPN

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Firewall > Access Rules**. Se abre la página *Regla de acceso*:

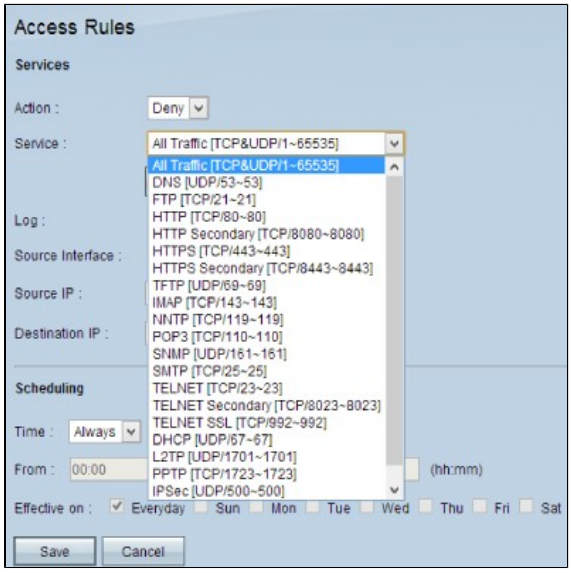


Nota: Las reglas de acceso predeterminadas no se pueden editar. Las reglas de acceso mencionadas en la imagen anterior, configuradas por el usuario, se pueden editar mediante el siguiente proceso.

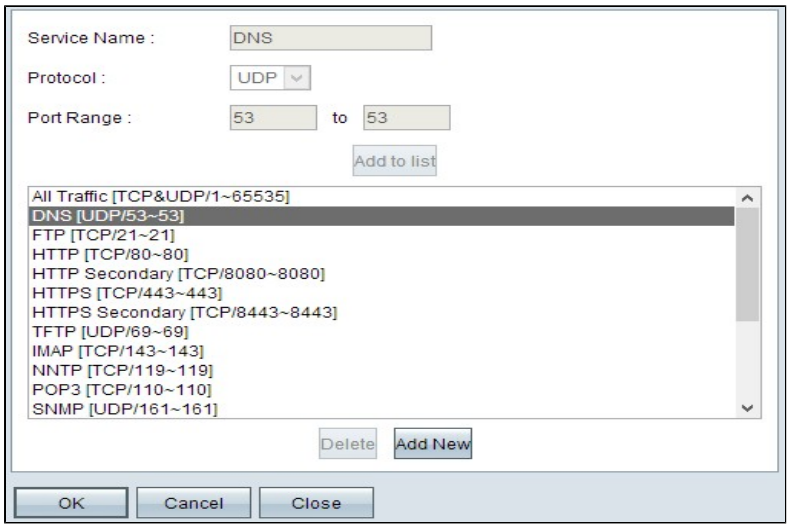
Paso 2. Haga clic en el botón **Agregar** para agregar una nueva regla de acceso. La página *Access Rules* cambia para mostrar las áreas Services y Scheduling. La adición de una regla de acceso se explica en los pasos siguientes.



Paso 3. Elija **Denegar** en la lista desplegable Acción para denegar el servicio.



Paso 4. Elija el servicio necesario que se aplica a la regla en la lista desplegable **Servicio**.



Paso 5. (Opcional) Para agregar un servicio que no esté presente en la lista desplegable de servicios, haga clic en **Administración de servicios**. En la Administración de servicios, se puede crear un servicio según sea necesario. Después de crear un servicio, haga clic en **Aceptar** para guardar la configuración.

Paso 6. Elija **Registrar paquetes que coincidan con esta regla** en la lista desplegable Registro sólo para registros que coincidan o **No registrar** para registros que no coincidan con la regla de acceso.

Paso 7. Elija un tipo de interfaz de la lista desplegable Interfaz de origen, que es el origen de las reglas de acceso. Las opciones disponibles son:

· LAN: Elija LAN si la interfaz de origen es la red de área local.

· WAN: Elija WAN si la interfaz de origen es el ISP.

· DMZ: Elija DMZ si la interfaz de origen es la zona desmilitarizada.

· ANY â€" Elija ANY para hacer la interfaz de origen como cualquiera de las interfaces mencionadas anteriormente.

Paso 8. En la lista desplegable IP de origen, elija las direcciones de origen que desee que se apliquen a la regla de acceso. Las opciones disponibles son:

· Single: seleccione Single si se trata de una única dirección IP e introduzca la dirección IP.

· Rango: elija Rango si se trata de un rango de direcciones IP e introduzca la primera y la última dirección IP del rango.

· ANY: elija ANY para aplicar las reglas a todas las direcciones IP de origen.

Paso 9. En la lista desplegable Destination IP (IP de destino), seleccione las direcciones de destino deseadas que se aplican a la regla de acceso. Las opciones disponibles son:

· Single: seleccione Single si se trata de una única dirección IP e introduzca la dirección IP.

· Rango: elija Rango si se trata de un rango de direcciones IP e introduzca la primera y la última dirección IP del rango.

· ANY: elija ANY para aplicar las reglas a todas las direcciones IP de destino.

Paso 10. Elija un método para definir cuándo están activas las reglas en la lista desplegable Hora. Las fallas son las siguientes:

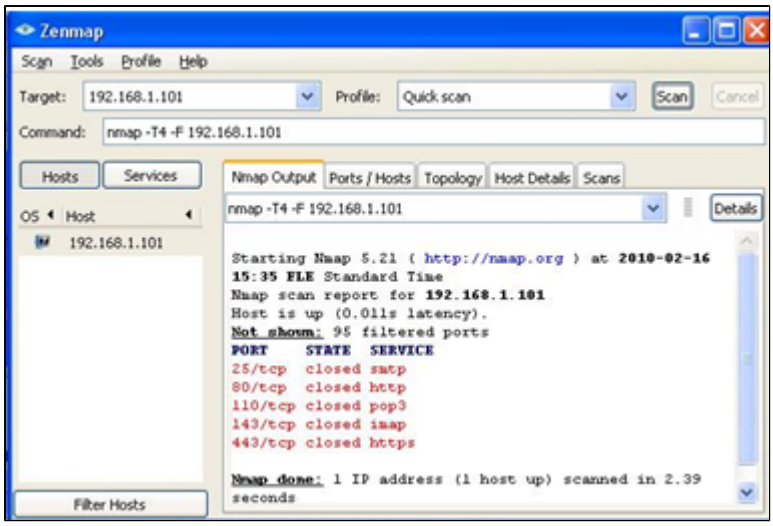
· Siempre: si selecciona Siempre en la lista desplegable Hora, las reglas de acceso se aplicarán siempre al tráfico.

· Intervalo: puede elegir un intervalo de tiempo específico en el que las reglas de acceso están activas si selecciona Intervalo en la lista desplegable Tiempo. Después de especificar el intervalo de tiempo, active las casillas de verificación de los días en los que desea que las reglas de acceso estén activas desde el campo Vigente el.

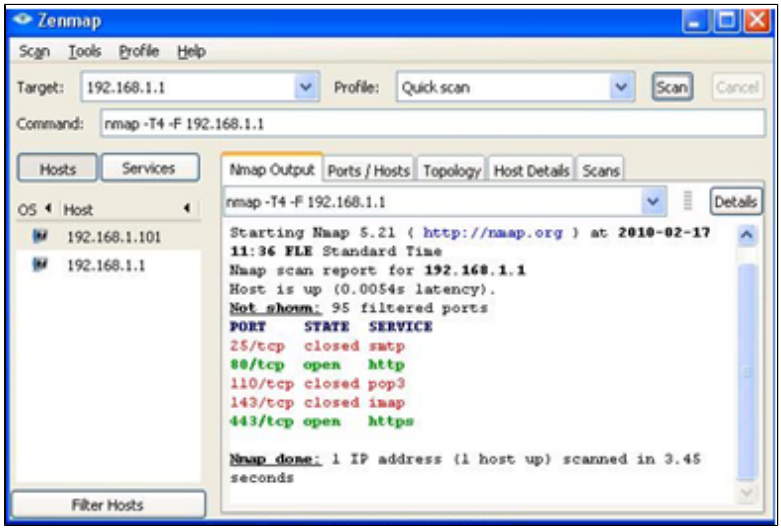
Paso 11. Haga clic en **Save** para guardar la configuración.

Paso 12. Repita los pasos del 2 al 10 con los campos que coincidan con los que se muestran en la imagen, respectivamente. Aquí se aplican las normas de acceso según el cliente. Los primeros 7 permiten algunos servicios; el 8 deniega el resto del tráfico. Esta configuración también se realiza en el segundo router. Se permite el puerto IPSec 500.

Nota: Haga esto para que ambos routers verifiquen que las reglas de acceso están configuradas según lo deseado.



Router VPN n.º 1

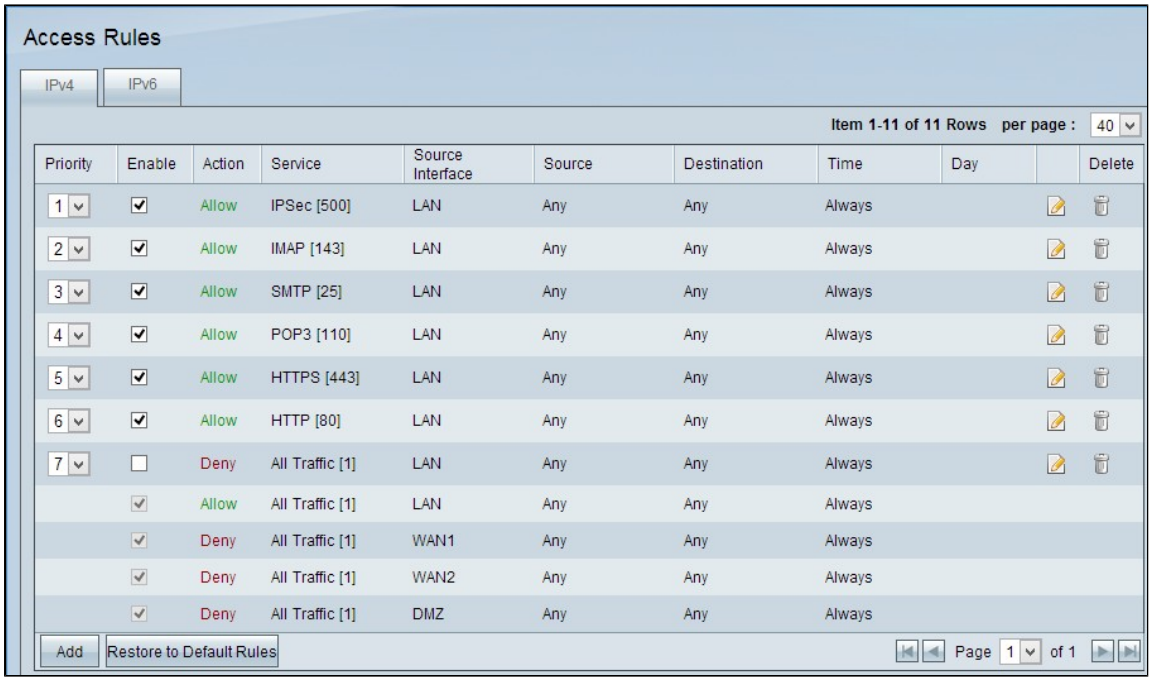


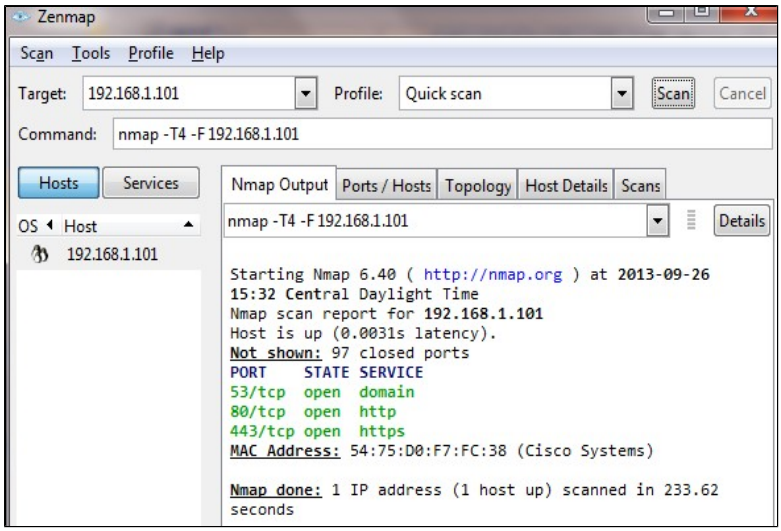
Router VPN n.º 2

Paso 13. Instale Zenmap(NMAP) desde http://nmap.org/download.html el y ejecútelo en una PC en la LAN 192.168.2.0.

Nota: Esta es la LAN detrás del router con las siete ACL adicionales. La IP de destino (192.168.1.101) es un PC de la LAN de gateway remoto.

Paso 14. Seleccione **Quick Scan** en el perfil y haga clic en **Scan**. A través de esto podemos conocer los puertos abiertos y filtrados según las ACL, el resultado mostrado se representa en la imagen de arriba. La salida muestra que estos puertos están cerrados, independientemente de las ACL permitidas que se configuran en el RV0xx # 1. Si intentamos verificar los puertos a la IP LAN (192.168.1.1) del gateway remoto, descubrimos que los puertos 80 y 443 están abiertos (que estaban cerrados al PC 192.168.1.101).





La ACL funciona correctamente después de la eliminación de la 7a ACL denegada y funciona correctamente como se puede ver en el resultado.

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).