

Configuración de ACL IP utilizadas frecuentemente

Contenidos

Introducción

Requisitos previos

- Requisitos
- Componentes utilizados
- Convenciones

Ejemplos de configuración

- Permiso de acceso a la red para un host seleccionado
- Negación del acceso a la red para un host seleccionado
- Permiso de acceso a un intervalo de direcciones IP contiguas
- Negación del tráfico Telnet (TCP, puerto 23)
- Permiso de inicio de sesión TCP sólo para redes internas
- Negación del tráfico FTP (TCP, puerto 21)
- Permiso de tráfico FTP (FTP activo)
- Permiso de tráfico FTP (FTP pasivo)
- Permiso de pings (ICMP)
- Permiso de HTTP, Telnet, Mail, POP3, FTP
- Permiso de DNS
- Permiso de actualizaciones de enrutamiento
- Depuración de tráfico basada en ACL

Verificación

Resolución de problemas

Introducción

En este documento se proporcionan ejemplos de configuraciones para listas de control de acceso (ACL) IP que se usan con frecuencia y que filtran paquetes IP en función de:

- La dirección de origen
- La dirección de destino
- El tipo de paquete
- Cualquier combinación de los elementos anteriores

Para filtrar el tráfico de red, las ACL controlan si los paquetes enrutados se reenvían o bloquean en la interfaz del router. El router examina cada paquete para determinar si debe reenviarlo o descartarlo según los criterios que se especifiquen dentro de la ACL. Los criterios de la ACL son:

- La dirección de origen del tráfico
- La dirección de destino del tráfico
- El protocolo de capa superior

Siga los pasos siguientes para generar una ACL como muestran los ejemplos de este documento:

1. Cree una ACL.
2. Aplique la ACL a una interfaz.

La ACL IP es una colección secuencial de condiciones de permiso y denegación que se aplica a un paquete IP. El router prueba los paquetes en relación con las condiciones en la ACL, uno por vez.