

Resolver problemas las configuraciones del Firewall Cisco IOS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona información que podrá utilizar para resolver problemas en las configuraciones de Cisco IOS® Firewall.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

[Troubleshooting](#)

Note: Consulte [información importante en los comandos debug](#) antes de ejecutar los comandos debug.

- Para invertir (quitar) una lista de acceso, ponga un “no” delante del **comando access-group** en el modo de configuración de la interfaz:

```
int <interface>
no ip access-group # in|out
```

- Si se niega demasiado tráfico, estudie la lógica de su lista o intente definir una lista más amplia adicional, y después aplíquela en lugar de otro. Por ejemplo:

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int <interface>
ip access-group # in|out
```

- **El comando show ip access-lists** muestra qué Listas de acceso son aplicadas y qué tráfico es negado por ellas. Si usted mira la cuenta de paquetes negada antes y después de que la operación fallada con el IP Address de origen y de destino, este número aumenta si la lista de acceso bloquea el tráfico.
- Si el router no se cargó completamente, la depuración puede hacerse a nivel del paquete en la lista de acceso de inspección ip o extendida. Si cargan al router pesadamente, el tráfico se reduce a través del router. Utilice la discreción con los comandos de debugging. Agregue temporalmente el **comando no ip route-cache a la interfaz**:

```
int <interface>
no ip route-cache
```

Entonces, en el modo del permiso (pero no config):

```
term mon
debug ip packet # det
```

produce la salida similar a esto:

```
term mon
debug ip packet # det
```

- Se pueden utilizar las listas de acceso extendidas con la opción "registro" al final de los distintos enunciados:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

Usted por lo tanto ve los mensajes en la pantalla para permitido y tráfico denegado:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

- Si el IP examina la lista es sospechada, el **comando debug ip inspect <type_of_traffic>** produce la salida tal como esta salida:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

Para estos comandos, junto con la otra información de Troubleshooting, refiera al [Proxy de autenticación del troubleshooting](#).

Información Relacionada

- [Soporte de productos del Firewall Cisco IOS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)