Solución de problemas de terminales Catalyst serie 9000 que no reciben dirección DHCP cuando ISE la redirige

Contenido

Problema

Después de habilitar la autenticación mediante la redirección de Cisco Identity Services Engine (ISE) en un switch Cisco Catalyst serie 9000, los terminales con cable no pueden obtener direcciones IP de forma intermitente a través del protocolo de configuración dinámica de host (DHCP). No se observan problemas en switches que no sean Catalyst serie 9000 y utilicen las mismas configuraciones.

Entorno

- Familia de productos: Catalyst serie 9000
- Equipos Windows que experimentan errores de adquisición DHCP
- La lista de control de acceso (ACL) de redirección en el switch Catalyst serie 9000 no deniega explícitamente el tráfico DHCP

Resolución

1. Agregue las siguientes sentencias deny a la ACL de redirección para manejar explícitamente el tráfico DHCP:

```
deny udp any eq bootps any
```

```
deny udp any any eq bootpc

deny udp any eq bootpc any
```

2. Después de modificar la ACL, vuelva a autenticar un dispositivo que fallaba anteriormente para verificar que ahora puede recuperar correctamente una dirección IP a través de DHCP.

Causa

Los switches Catalyst de la serie 9000 procesan paquetes de manera diferente que los modelos de switches más antiguos cuando se habilita la autenticación. El orden de procesamiento de paquetes en los switches Catalyst de la serie 9000 es el siguiente:

1. Los paquetes que coinciden con una regla permit Access Control Entry (ACE) se envían a la CPU para su redirección al servidor AAA.

2. Los paquetes que coinciden con una regla ACE de negación se reenvían a través del switch.

3. La siguiente lista de control de acceso descargable (DACL) procesa los paquetes que no coinciden con las reglas ACE de permiso o denegación y, si no existe ninguna DACL, los paquetes llegan a la ACL de denegación implícita y se descartan.

Este método de procesamiento difiere de los modelos de switch anteriores que utilizan ACL predeterminadas que permiten el tráfico DHCP de forma predeterminada y se procesan antes de redirigir las ACL. Los modelos de la serie Catalyst 9000 no utilizan estas ACL predeterminadas y, en su lugar, dependen completamente de la ACL de redirección y la DACL en la sesión. La ACL predeterminada para sesiones de modo cerrado en switches Catalyst predecesores es la siguiente:

```
3750#sh ip access-lists Auth-Default-ACL

Extended IP access list Auth-Default-ACL

    10 permit udp any range bootps 65347 any range bootpc 65348 (22 coincidencias)

    20 permit udp any any range bootps 65347 (12 coincidencias)
```

```
30 deny ip any any
```

Contenido relacionado

- ACL predeterminadas para autenticación 802.1X
- Soporte técnico y descargas de Cisco

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).