排除Catalyst 9000系列终端在ISE重定向时无法接收DHCP地址的问题

目录

问题

在Cisco Catalyst 9000系列交换机上使用来自思科身份服务引擎(ISE)的重定向启用身份验证后，有线终端间歇性地无法通过动态主机配置协议(DHCP)获取IP地址。在使用相同配置的非Catalyst 9000系列交换机上未发现任何问题。

环境

- 产品系列：Catalyst 9000系列
- 发生DHCP获取故障的Windows计算机
- Catalyst 9000系列交换机上的重定向访问控制列表(ACL)不会明确拒绝DHCP流量

分辨率

1.将以下deny语句添加到重定向ACL以显式处理DHCP流量：

```
deny udp any eq bootps any

deny udp any any eq bootpc

deny udp any eq bootpc any
```

2.修改ACL后，重新验证之前出现故障的设备，以验证它现在是否可以通过DHCP成功检索IP地址。

原因

启用身份验证时，Catalyst 9000系列交换机处理数据包的方式与旧交换机型号不同。Catalyst 9000系列交换机上的数据包处理顺序如下：

1.将与permit Access Control Entry(ACE)规则匹配的数据包发送到CPU以重定向到AAA服务器。

2.与拒绝ACE规则匹配的数据包将通过交换机转发。

3.既不匹配允许也不匹配ACE规则的数据包由下一个可下载访问控制列表(DACL)处理，如果没有DACL，则数据包会命中隐式 — 拒绝ACL并被丢弃。

此处理方法与使用默认ACL的较旧交换机型号不同，这些默认ACL默认允许DHCP流量，在重定向ACL之前进行处理。Catalyst 9000系列型号不使用这些默认ACL，而是完全依赖于会话上采用的重定向ACL和DACL。前身Catalyst交换机上关闭模式会话的默认ACL如下：

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

扩展IP访问列表Auth-Default-ACL

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

    20 permit udp any any range bootps 65347（12个匹配）

    30 deny ip any any
```

相关内容

- 802.1X身份验证的默认ACL
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。