MSR V7 802.1X支持快速EAD快速部署限制

802.1X MAC地址认证 罗燕 2020-02-21 发表

问题描述

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中EAD客户端的部署工作量很大，例如，需要网络管理员手动为每一个EAD客户端下载、升级客户端软件，这在EAD客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X认证支持的EAD快速部署功能就可以解决以上问题，它允许未通过认证的802.1X用户访问一个指定的IP地址段（称为Free IP），并可以将用户发起的HTTP访问请求重定向到该IP地址段中的一个指定的URL（重定向URL），实现用户自动下载并安装EAD客户端的目的。

· Free IP：未通过认证的802.1X终端用户可以访问的IP地址段，该IP地址段中可以配置一个或多个特定服务器，用于提供EAD客户端的下载升级或者动态地址分配等服务。

· 重定向URL：802.1X终端用户在认证成功之前，如果使用浏览器访问网络，则设备会将用户访问的URL重定向到已配置的URL（例如，重定向到EAD客户端下载界面），这样只要用户打开浏览器，就必须进入管理员预设的界面。

EAD快速部署功能通过制订EAD规则（通常为ACL规则）来给予未通过认证的终端用户受限制的网络访问权限。当大量用户同时认证时，ACL资源将迅速被占用，如果没有用户认证成功，将出现ACL资源不足的情况，会导致一部分新接入的用户无法认证。

管理员可以通过配置EAD规则的老化时间来控制用户对ACL资源的占用，当用户访问网络时该定时器开始计时，在定时器超时或者用户下载客户端并成功通过认证之后，该用户所占用的ACL资源被删除，在老化时间内未进行任何操作的用户所占用的ACL资源会及时得到释放。

那我们部署的时候有什么注意事项呢?

解决方法

· MAC地址认证和端口安全特性不支持EAD的快速部署功能，全局使能MAC认证或端口安全功能将会使EAD快速部署功能失效。

· 为使EAD快速部署功能生效，必须保证指定端口的授权模式为auto。

· MAC地址认证、端口安全功能均与Free IP配置互斥。

· 开启EAD快速部署辅助功能与802.1X Guest VLAN功能不建议同时配置，否则可能导致802.1X Guest VLAN功能无法正常使用。

· 在同时配置了Free IP与Auth-Fail VLAN功能的情况下，请保证Free IP网段为Auth-Fail VLAN可允许访问的网络资源。这种情况下，用户只能访问Free IP，不能访问其它资源。

· 未通过802.1X认证的用户若要通过外网的DHCP服务器动态获得IP地址，则需要保证该DHCP服务器的IP地址在配置的Free IP内。

· 重定向URL必须处于Free IP网段内，否则无法实现重定向。