CPPM 对接 AD，无法使用 AD 账号实现 1X 认证

By CCE

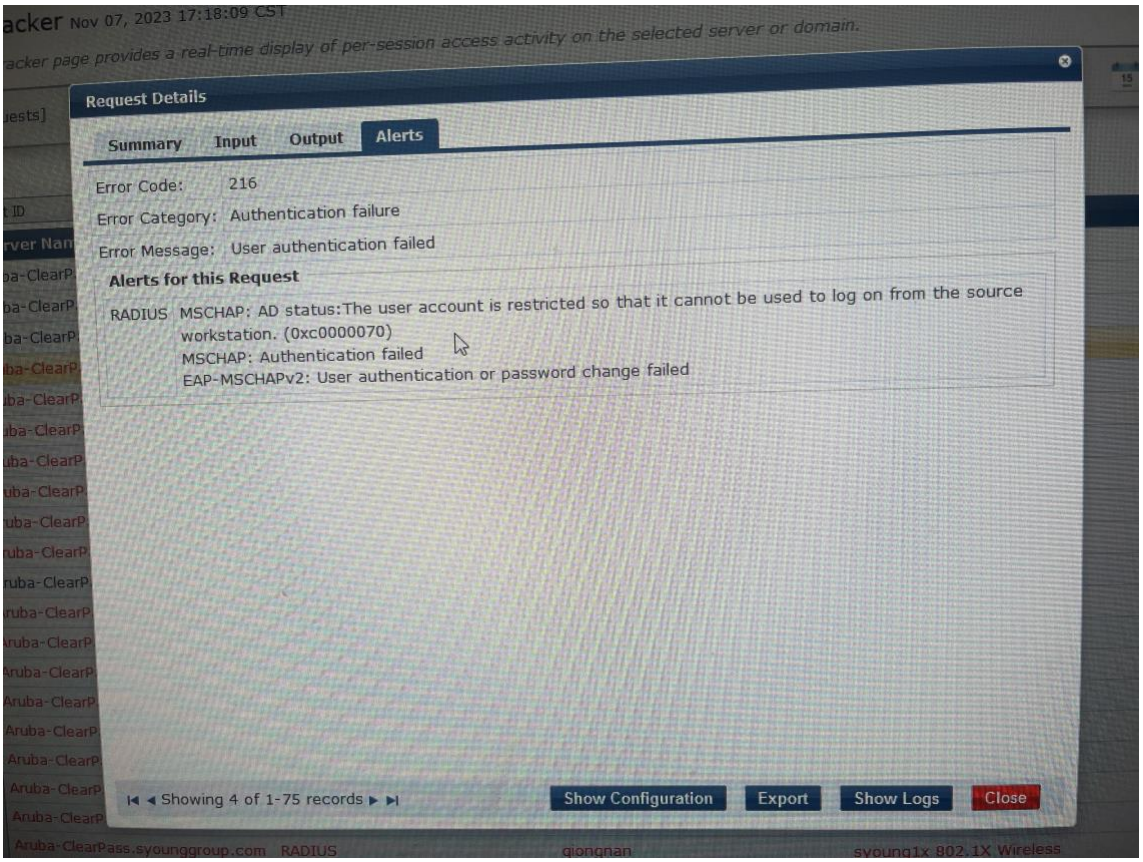
现象描述:

CPPM v6.11.1， 采用加入 AD 域的方式来实现终端的 802.1x 认证(采用 EAP-PEAP 认证方法)，无论是加域的终端还是非加域终端，在用户认证阶段失败。

在 Access Tracker 的 Alerts 选项卡中提示

MSCHAP:AD status:The user account is restricted so that it cannot be used to log on from the source workstation.(0xc0000070)

错误信息截图如下:



问题原因:

这里报错的根本原因是 AD 上针对该账号开启了登录到功能，要求该账号只能在指定的计算机名称主机上实现管理员登陆， 如果该账号在其他的主机上登陆(该主机的 Hostname 不包含在登录到的 计算机名称列表中)， 那么 AD 是阻止其登陆权限的。

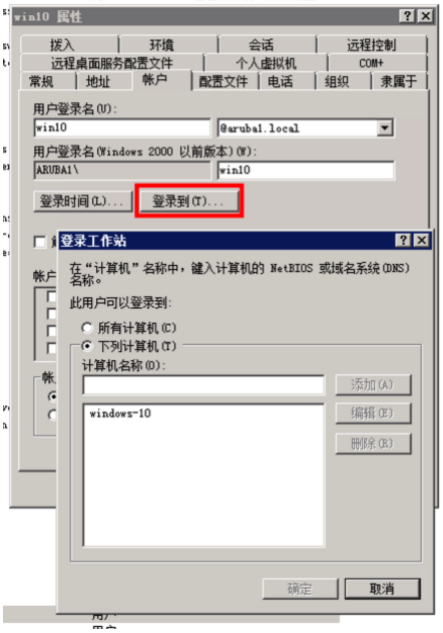
那我们用的加域终端本身就是该账号的登录到的指定计算机名称，为什么也是无法登录呢?

原因就是在基于 AD 认证源的场景中，CPPM 采用 Join Domain 方式结合本地的 Samba 服务，能够基于域控制器来认证 AD 域的用户.CPPM 在这个过程中会使用自己的主机名向域控制器发送 user name，Challenge 和 response，如果认证成功，AD 会返回 NT Key 给到 CPPM。

此时 AD 会认为该账号正登录到 CPPM 的主机名上，而 AD 中的该账号 的登录到中的计算机名称中没有 CPPM 的 Hostname。

Ad 的账号有个 登录到 属性， 一旦开启，设置为该用户可以登录到指定的计算机名称的主机上，不在该列表中的其他主机上是不能使用该账号登录的。

参考链接 https://blog.csdn.net/weixin_42493507/article/details/123247562

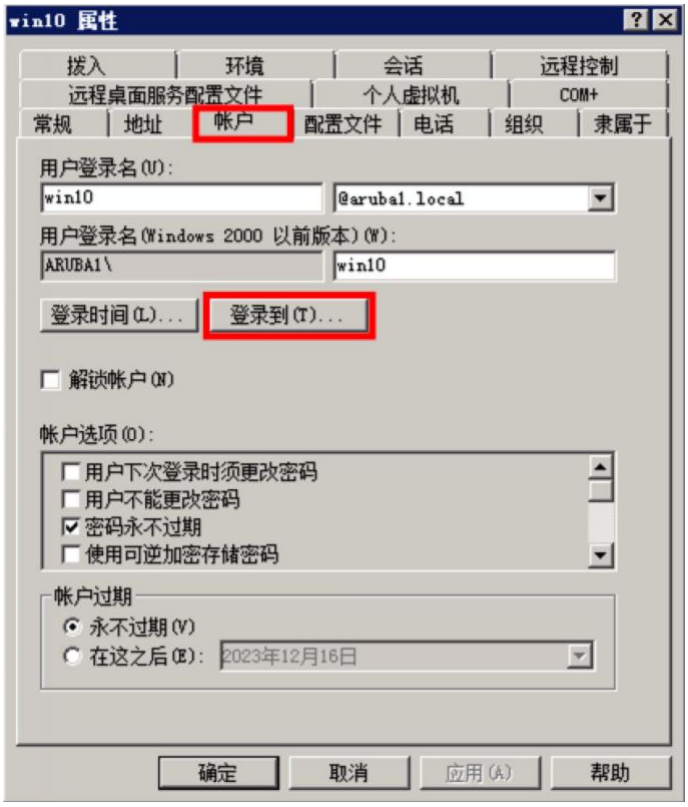


解决办法:

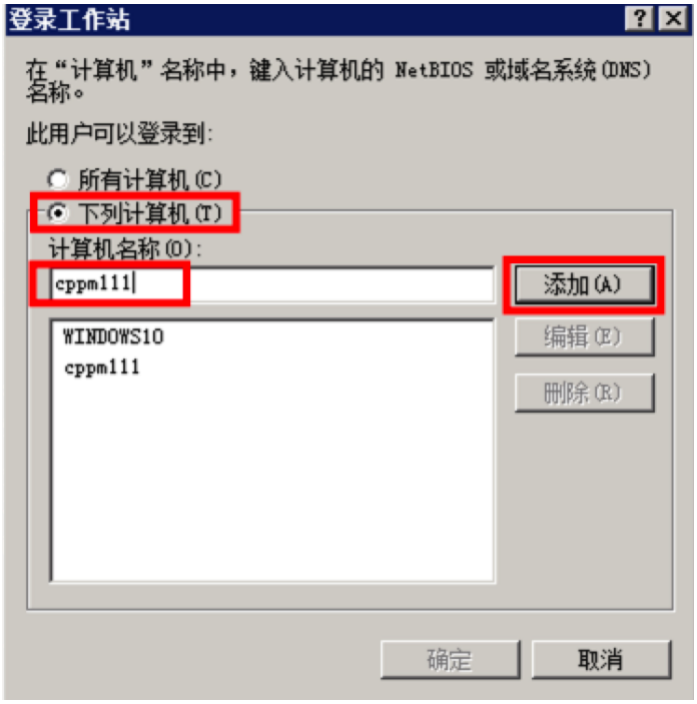
1. 在 AD 的每个账号的登录到的计算机名称中，增加 CPPM 的 Hostname。因为如果客户使用该功能，那必然会针对每个账号所允许登录到的计算机名称是经常维护和变更的。
    i. 该方法不需要额外地在 AD 上开启 NPS 服务，降低操作的复杂性。
    ii. 此时还是 CPPM+AD 认证源的方式， 终端的信任 EAP 证书仍然是 CPPM RADIUS/EAP 服务器证书(强烈建议使用本地的 Onboard root ca 来签发一张私签的 RADIUS/EAP 服务器证书并导入到 CPPM 中)。
    iii. 终端的用户认证和机器认证需要提前在 Trusted Root Certification Authorities-受信任的根证书颁发机构中导入 CPPM Onboard root ca。

以下是 AD 账号的登录到的配置步骤截图:

1) 在 AD 中找到指定的登录账号，然后鼠标双击下该账号，进入到账号属性界面，点击账户选项卡，点击 登录到 按钮

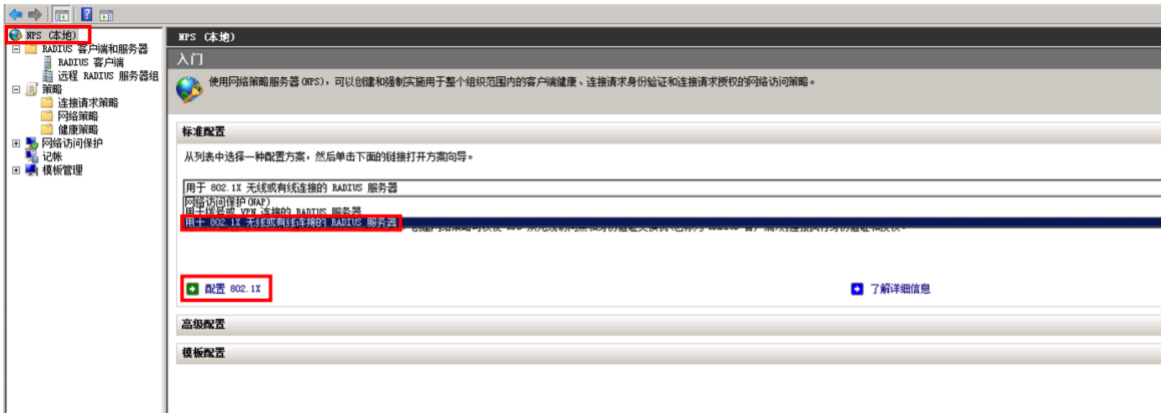


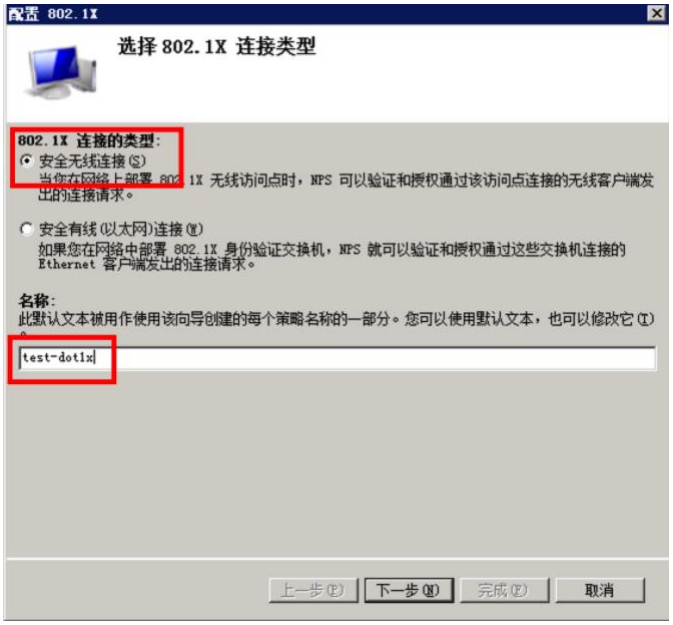
2) 在登录到界面，在计算机名称中输入 CPPM Hostname， 点击添加按钮，最后点击确定按钮



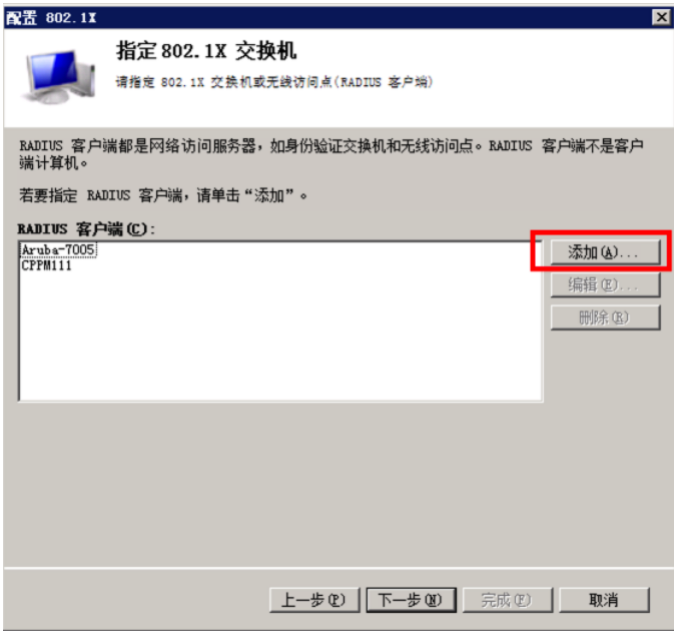
2. 如果客户的终端数量多，且不想在每个终端的登录到的计算机名称中变更，那我们可以在 AD 上启用 NPS 服务并配置 ADCS. 利用 AD 的 NPS 服务来实现 1X 认证，从而绕过了 登录到的指定计算机名称的限制，NPS RADIUS 需要 EAP 证书，同时开启用户认证组和机器认证组.实现的拓扑就是 无线接入-→CPPM-→ NPS(AD)，认证源要变成 RADIUS Server 指向 NPS， CPPM 作为 RADIUS Proxy。

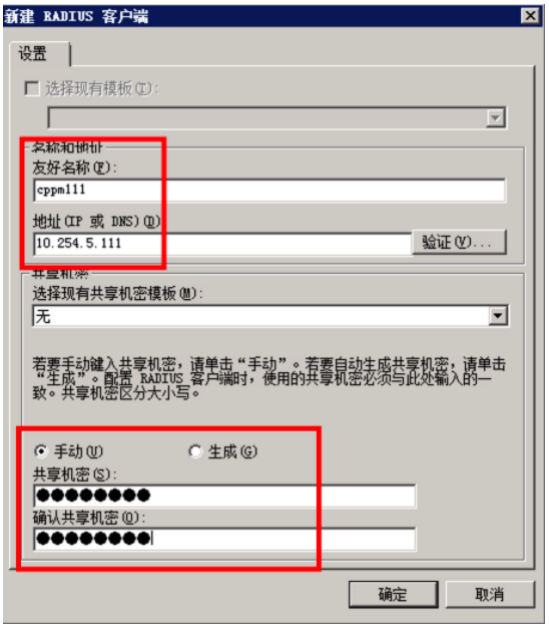
以下是 AD 上如何启用 NPS 服务的配置步骤截图:

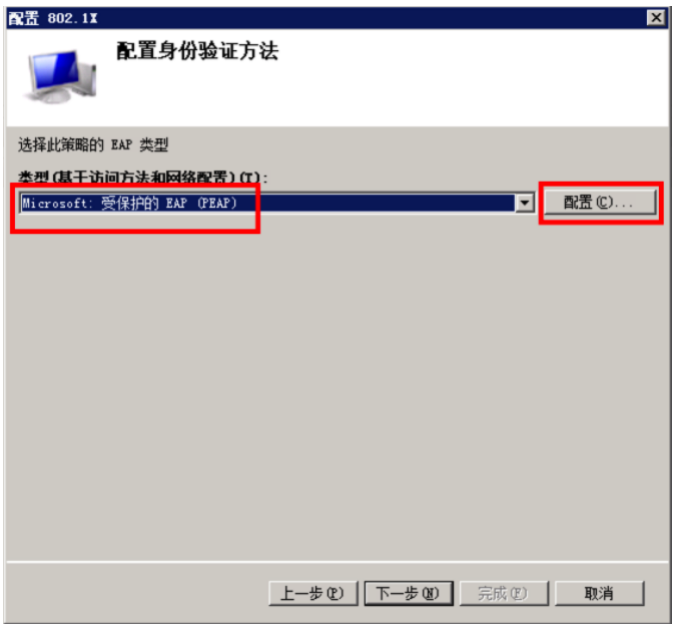




对于 NPS 来说， RADIUS Client 是 CPPM，所以要添加 CPPM 信息。





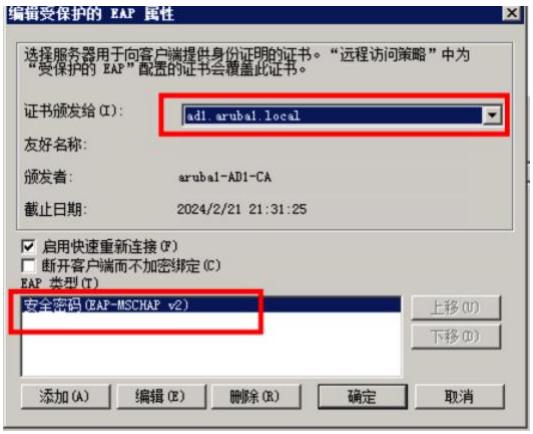


这里调用的证书就是 EAP 证书，也叫做 RADIUS/EAP 服务器证书。

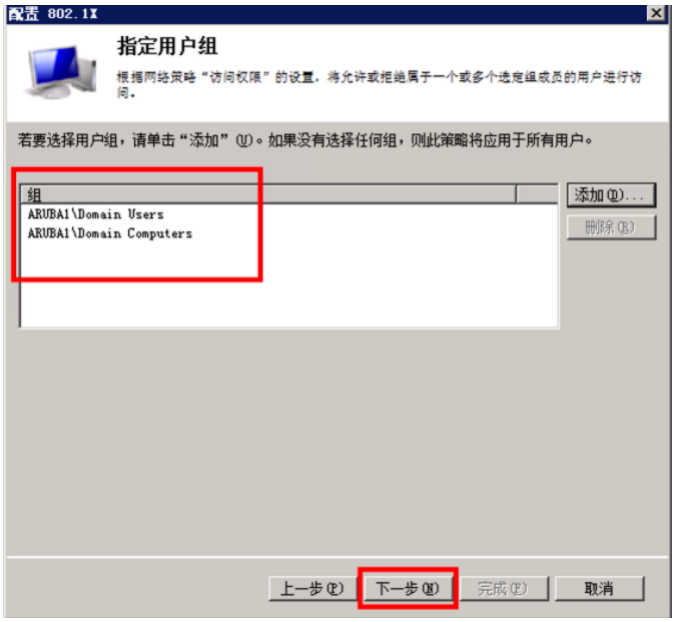
实际上是 ADCS 签发给 NPS 的服务器证书。

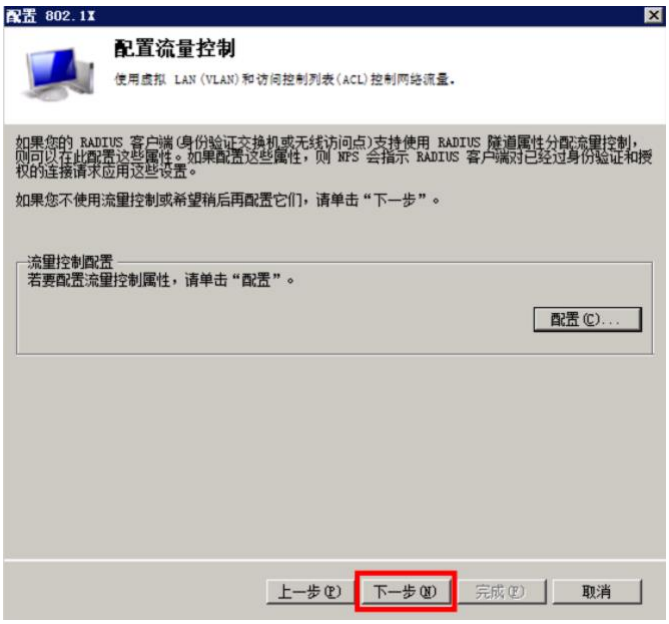
由 NPS 在 MMC 的机器账号的个人证书中创建 CSR， 然后由 ADCS 签发一张 RADIUS/EAP 服务器证书， 然后在 NPS 上下载并安装该服务器证书(实际就是导入该证书，存储的位置在 Local Machine 的 Personal 中)。

详细的配置步骤参考 : https://arubase.club/archives/6422

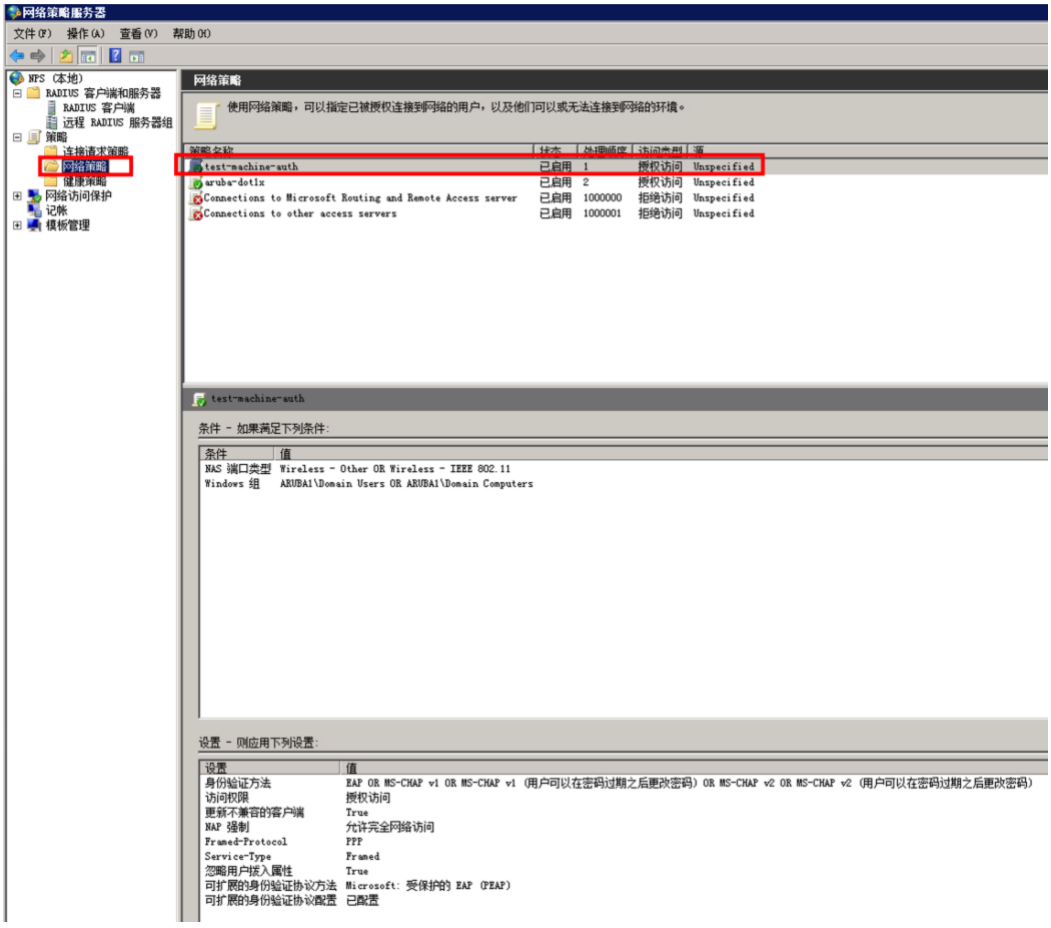


在 NPS 上同时开启用户认证的用户组和机器认证的用户组


配置 802.1X
指定用户组
根据网络策略“访问权限”的设置，将允许或拒绝属于一个或多个选定组成员的用户进行访问。
若要选择用户组，请单击“添加”(U)。如果没有选择任何组，则此策略将应用于所有用户。
组
ARUBA1\Domain Users
ARUBA1\Domain Computers
添加(D)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消


配置 802.1X
配置流量控制
使用虚拟 LAN (VLAN)和访问控制列表(ACL)控制网络流量。
如果您的 RADIUS 客户端(身份验证交换机或无线访问点)支持使用 RADIUS 隧道属性分配流量控制，则可以在此配置这些属性。如果配置这些属性，则 NPS 会指示 RADIUS 客户端对已经过身份验证和授权的连接请求应用这些设置。
如果您不使用流量控制或希望稍后再配置它们，请单击“下一步”。
流量控制配置
若要配置流量控制属性，请单击“配置”。
配置(C)...
上一步(P)
下一步(N)
完成(F)
取消

最后就是调整你创建好的网络策略的匹配顺序。



在 CPPM 上创建认证源，类型是 RADIUS 的，指向 NPS， 然后在你需要的认证 service 中调用该认证源.