计算机访问限制的优缺点

目录

简介

本文档介绍计算机访问限制(MAR)遇到的问题，并提供了解决该问题的解决方案。

随着个人拥有设备的增长，系统管理员必须始终提供一种方法，将对网络某些部分的访问限制为仅对公司拥有的资产进行访问。本文档中描述的问题涉及如何安全地识别这些关注领域并对其进行身份验证，而不会中断用户连接。

先决条件

要求

思科建议您了解802.1x，以便全面了解本文档。本文档假定您熟悉用户802.1x身份验证，并重点介绍与使用MAR（更一般地说，是机器身份验证）相关的问题和优势。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

MAR基本上尝试解决大多数当前和流行的可扩展身份验证协议(EAP)方法所固有的一个常见问题，即机器身份验证和用户身份验证是独立的、不相关的过程。

用户身份验证是大多数系统管理员熟悉的802.1x身份验证方法。其思想是，凭证（用户名/密码）会

提供给每个用户，而这组凭证代表一个物理人员（也可以在多个人之间共享）。 因此，用户可以使用这些凭证从网络中的任何位置登录。

计算机身份验证在技术上是相同的，但通常不会提示用户输入凭证（或证书）；计算机或机器自行完成。这要求计算机已存储凭据。发送的用户名**是host/<MyPCHostname>**，前提是您的计算机已将**<MyPCHostname>**设置为主机名。换句话说，它发送主机**/后跟**主机名。

虽然与Microsoft Windows和Cisco Active Directory不直接相关，但如果计算机加入Active Directory，则此过程会更容易呈现，因为计算机主机名已添加到域数据库，并且凭证会协商（默认情况下每30天更新一次）并存储在计算机上。这意味着可以从任何类型的设备进行计算机身份验证，但是，如果计算机加入Active Directory，并且凭据对用户隐藏，则可更轻松、透明地进行身份验证。

MAR即解决方案

很容易说，该解决方案是思科访问控制系统(ACS)或思科身份服务引擎(ISE)完成MAR，但实施之前需要考虑其优缺点。如何实施这一点在ACS或ISE用户指南中进行了最好的描述，因此本文档简单介绍了是否要考虑这一点以及一些可能的障碍。

优点

MAR是由于用户和机器身份验证完全分离而发明的。因此，RADIUS服务器无法实施用户必须从公司拥有的设备登录的验证。使用MAR时，RADIUS服务器（思科端的ACS或ISE）对于给定用户身份验证强制在X小时（通常为8小时，但是这是可配置的）内必须有有效的机器身份验证，在对同一终端进行用户身份验证之前。

因此，如果RADIUS服务器知道计算机凭证（通常是计算机加入域），并且RADIUS服务器通过与域的连接来验证此身份验证，则计算机身份验证成功。网络管理员完全需要确定成功的计算机身份验证是提供对网络的完全访问，还是仅提供受限访问；通常，这至少会打开客户端与Active Directory之间的连接，以便客户端可以执行诸如更新用户密码或下载组策略对象(GPO)之类的操作。

如果用户身份验证来自在过去几小时内未进行计算机身份验证的设备，则会拒绝用户，即使用户通常有效。

仅当身份验证有效且从过去几小时内发生计算机身份验证的终端完成时，才向用户授予完全访问权限。

缺点

本节介绍MAR使用的缺点。

MAR和Microsoft Windows请求方

MAR的思想是，要完成用户身份验证，不仅用户必须具有有效凭证，而且必须从该客户端记录成功的计算机身份验证。如果存在任何问题，用户将无法进行身份验证。出现的问题是，此功能有时可能会无意中锁定合法客户端，这会迫使客户端重新启动以重新获得对网络的访问。

Microsoft Windows仅在启动时（当出现登录屏幕时）执行计算机身份验证；一旦用户输入用户凭证，就执行用户身份验证。此外，如果用户注销（返回登录屏幕），则执行新的计算机身份验证。

以下示例场景显示了MAR有时导致问题的原因：

用户X整天使用笔记本电脑，笔记本电脑通过无线连接连接。一天结束时，他只是关上笔记本电脑，然后停工。这会使笔记本电脑进入休眠状态。第二天，他回到办公室，打开笔记本电脑。现在，他无法建立无线连接。

当Microsoft Windows休眠时，它会获取系统当前状态的快照，包括登录者的上下文。用户笔记本电脑的MAR缓存条目在一夜之间过期并清除。但是，当笔记本电脑通电时，它不执行计算机身份验证。它直接进入用户身份验证，因为休眠过程就记录了这一点。解决此问题的唯一方法是注销用户或重新启动计算机。

虽然MAR是一项好功能，但它有可能导致网络中断。在您了解MAR的工作方式之前，这些中断很难排除；实施MAR时，必须向最终用户说明如何在每天结束时正确关闭计算机并注销每台计算机。

MAR和各种RADIUS服务器

在网络中有多台RADIUS服务器以实现负载均衡和冗余目的是很常见的。但是，并非所有RADIUS服务器都支持共享MAR会话缓存。仅ACS版本5.4及更高版本和ISE版本2.3及更高版本支持节点之间的MAR缓存同步。在这些版本之前，无法对一个ACS/ISE服务器执行计算机身份验证，也无法对另一个服务器执行用户身份验证，因为它们彼此不对应。

MAR和有线 — 无线交换

许多RADIUS服务器的MAR缓存依赖于MAC地址。它只是一个表，其中包含笔记本电脑的MAC地址和最后一次成功的计算机身份验证的时间戳。这样，服务器就能知道客户端在过去X小时内是否通过计算机身份验证。

但是，如果您使用有线连接启动笔记本电脑（因此从有线MAC执行计算机身份验证），然后在白天切换到无线，会发生什么情况？RADIUS服务器无法将您的无线MAC地址与您的有线MAC地址关联，并且无法知道您在过去X小时内已经过计算机身份验证。唯一的方法是注销并让Microsoft Windows通过无线进行另一台计算机身份验证。

解决方案

Cisco AnyConnect具有预配置配置文件的优势，可触发计算机和用户身份验证。但是，与Microsoft Windows请求方一样，也遇到了仅在注销或重新启动时才发生计算机身份验证的限制。

此外，使用AnyConnect版本3.1及更高版本，可以使用EAP链执行EAP-FAST。这基本上是单一身份验证，其中您同时发送两对凭证，即计算机用户名/密码和用户用户名/密码。然后，ISE会更轻松地检查两者是否都成功。由于没有使用缓存，也无需检索以前的会话，因此可提供更高的可靠性。

当PC启动时,AnyConnect仅发送计算机身份验证，因为没有可用的用户信息。但是，当用户登录时，AnyConnect会同时发送计算机和用户凭据。此外，如果断开或拔掉/重新插接电缆，则计算机和用户凭据将再次以单个EAP-FAST身份验证形式发送，这与早期版本的AnyConnect不使用EAP链接时不同。

EAP-TEAP是长期最佳解决方案，因为它特别用于支持这些类型的身份验证，但是，从今天起，许多操作系统的本地请求方仍不支持EAP-TEAP