Cisco资格认证:思科NAC架构不简单Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022_Cisco_E8_B5_84_E6_A0_c101_557881.htm Cisco的NAC Framework是设计用来如何让多种硬件和软件组件协同工作，共同保护用户网络免受不良客户端侵害的一种架构。这些不良的客户端可能是没有及时打补丁的个人电脑，没有安装杀毒软件或者没有安装防火墙的电脑。ZDNet Solution的目的在于尽可能将复杂的NAC Framework架构浅显的介绍给大家。 什么是Cisco NAC Framework的组件? Cisco的NAC Framework试图解决一个复杂的问题，因此它必然也是一个复杂的解决方案。充分实施NAC Framework并不是一个简单的任务，因为整个架构中有太多来自Cisco和其它厂商的不同组件了，比如架构中包含了NAC策略管理器，多网络系统，认证服务器，补丁修补服务器，以及第三方安全软件验证服务器等。图A显示了整个框架的组件工作方式： 图A NAC架构工作方式 关于Cisco NAC Framework 不论是对于安全管理人员还是网络管理人员来说，让上图中的所有组件都和谐的工作，确实不是一件易事。不过没关系，思科的NAC架构已经被大多数主流终端安全公司，安全接入网关以及补丁修复服务器所支持。 Cisco NAC Framework如何工作 说了这么多，Cisco NAC Framework到底能做什么呢？以下是它的工作内容： 1.如果一台PC试图接入网络，首先必须经过验证，并且审核它的策略是否与规定相符。PC试图登录的行为会触发NAC过程。 2.PC主机运行思科可信代理Cisco Trust Agent (CTA). 3.网络接入设备Network Access Device (NAD) 即以太网交换机试图建立到PC机的连接

。 4.可扩展认证协议Extensible Authentication Protocol (EAP)启用，PC电脑上的凭据被发送到思科安全接入控制服务器上Cisco Secure Access Control Server (ACS)。 5.直到这整个过程完成，PC主机（潜在的不良终端）只是将来自可信代理Cisco Trust Agent的凭证发送到了网络上。PC机本身还不能与网络进行通信。 6.可信代理Cisco Trust Agent是通过一个安全通道传达凭证的，因此NAD看不到它们。 7.安全接入控制服务器ACS Server可以将凭证传递给其它的服务器。比如，现在大部分此类凭证都会发送给Windows AD服务器。当然，凭证也会发送给其它服务器，比如LDAP或一次性密码服务器。 8.根据一个或多个验证服务器反馈的信息，ACS服务器可以允许，拒绝或者隔离请求接入网络的PC。另外，ACS服务器可以设定不同的网络接入等级。 9.在校验安全策略一致性方面，Cisco NAC Framework采用的是网络和基于代理的扫描方式。 10.Cisco NAC Framework可以实施针对各类设备的一致性检测。 11.Cisco NAC Framework可以通知用户的连接状态，如果其中出现任何问题，它可以通过升级PC机的补丁，防火墙或其它设置等方式纠正所出现的问题。另外，也可以通过弹出窗口或类似功能通知PC机是否获得了网络访问权。比如用户可能会看到一个弹出窗口，其中标注为：“ 由于你的电脑缺少必要的升级补丁，因此没有获得网络访问权限。为了获得网络访问权限，请先访问以下地址[URL]获取电脑升级补丁。 ”图B可以帮助我们更好的理解这个过程： 图B连接过程 可能你注意到了，通常都是使用802.1X网络验证协议来验证试图接入网络的设备。因此NAD连接的交换机必须支持802.1X，否则该设备在验证和扫描前无法真正被隔离。

Cisco NAC Framework的组件都是什么? 知道了架构的大致工作方式，我们接下来逐一了解NAC框架的组件。以下就是组件和他们的功能介绍: 1.属性集Posture:这是试图接入网络的电脑所拥有的一系列凭证和属性的集合。包含了用户电脑的状态或健康程度，以及电脑上安装的程序信息。 2.思科可信代理Cisco Trusted Agent: Cisco Trusted Agent (CTA) 是Cisco NAC Framework的一个内部组件。CTA也被称作posture代理。 Cisco Trusted Agent其实是一个软件客户端，主要作用就是收集来自终端设备（NAD）上所安装的安全软件发来的状态信息。另外，它还会将接收到的“ posture ”（或者其它接收到的信息）传送给Cisco ACS Policy Server。 这里需要提一下，Cisco Trusted Agent只能与那些Cisco合作伙伴出品的NAC设备进行通信。目前市场上大概有50个厂商支持NAC。包括一线的补丁管理厂商，客户端安全产品厂商以及反病毒软件厂商。 3.网络接入设备Network Access Devices (NAD): NAD简单来讲就是PC机所连接的交换机。当然，它也有可能是路由器，VPN集线器，或者其它类似的网络接入设备。大部分厂商的交换机都支持Cisco NAC Framework。 4.AAA Policy Server: AAA策略服务器就是安全接入控制服务器Cisco Secure Access Control Server (ACS)。ACS服务器的主要功能是作为NAC部署的策略决策点。除此以外，Cisco Secure Access Control Server还评估用户的可信性以及网络终端的安全状态。 一般来说，Cisco Secure ACS Server会给Cisco接入设备发送每个用户的审核，包括可下载的访问控制列表。如果你没有使用Cisco的接入设备也不用担心，因为Cisco Secure Access Control Server还是会正常工作。 Cisco ACS Server是Cisco的一套应用程序，

可以运行在Windows或Linux Server上。ACS servers的管理范围相当大，就算没有NAC，Cisco ACS系统也还是可以作为RADIUS中心或TACACS 服务器。一般情况下，Cisco Secure Access Control Server管理验证，审核以及对访问网络控制信息的用户进行验证。 Cisco Secure Access Control Server的最大优势是它给管理员提供了控制用户访问网络的权利。另外还可以针对不同的用户控制使用不同的网络服务。如果想记录所有网络用户的所有行为， Cisco Secure Access Control Server也可以轻松实现。 5.目录服务器Directory Servers: Directory Servers提供用户ID，审核特权以及将成员信息分组。 6.属性认证服务器Posture Validation Server:正如我们刚才提到的，Cisco Secure Access Control Server可以将试图接入的系统的状态数据传送给程序指定的状态确认服务器，这一般是第三方厂商提供的。Posture Validation Server会判断终端设备的相关状态是否达标。根据Posture Validation Server的评估，Cisco Secure Access Control Server会对用户访问网络的请求做出允许或者拒绝的处理。 7.补丁修复服务器Remediation Servers: 补丁修复服务器的作用是保持设备符合一致性要求。它的最大好处是可以像Web服务器一样支持软件直接下载。另外，补丁修复服务器还可以自动评估设备以及提供软件升级补丁。 总结 Cisco 的NAC Framework是设计用来如何让多种硬件和软件组件协同工作，共同保护用户网络免受不良客户端侵害的一种架构。虽然整个框架使用起来不如Cisco NAC Appliance简单，但是却提供了包括很多第三方安全公司所提供的多种功能。因此，我们应该熟悉Cisco NAC Framework中的组件，包括可信代理 (Cisco Trust Agent), 安全接入控制服务器 (Cisco

ACS Server), 网络接入设备(NAD)即Cisco交换机，以及补丁修复服务器（用户在这里获取防火墙，操作系统或者杀毒软件所需的升级补丁）。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com