年度回顾:构建安全网络框架思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_B9_B4_E5_BA_A6_E5_9B_9E_E9_c101_644350.htm 1、信息安全到底是什么 刚刚我们了解了网络攻击的方式和手段。现在我们和大家一起看看，面对网络中无所不在的威胁和攻击，我们需要一个怎样的信息安全框架来进行整体防御。 我们一直在强调网络中信息安全的重要性。那么，我们是否能对信息安全做出一个明确的描述和定义呢?什么是信息?什么是信息安全? 首先，信息来源于数据，又不同于数据。数据是对事物或事件的客观描述，强调客观性.而信息是在数据的基础上，通过主观认识对其进行逻辑加工后的产物。一个强调客观描述，一个强调主观认识。当然，信息是不能脱离客观事实的，不符合事实的信息是错误的，需要修正的。 弄明白了信息的定义，我们来看看什么是信息安全。大家知道，信息很大程度上的价值增值是在于传递，而在信息传递过程中，通常需要满足三个要素的要求，也就是我们常说的信息安全三要素：保密性、完整性、可用性。 首先，要保证信息的完整的，不能在传递中丢失，其次，要保证信息除了既定接收者之外，不被其他人获取和破译，最后，要保证传递的信息是可用的，有价值的。满足了这三个要求，也就保证了信息的安全。 2、网络与端点，我该在哪里部署安全措施 我们知道，当信息流转在网络里时，有两个逻辑单元在保证信息的传递，一个是端点，一个是网络。信息就是从一个主机或客户端(端点)传递到路由器、、交换机、防火墙(网络)。这时候，信息安全保护可以在端点做，也可以在网络做。在端点做，可以将

攻击控制在源头，在网络做，可以做到风险的集中可控。 下面我们详细讨论一下两种安全策略的特点。在端点做防护，首先要保证端点本身不是恶意的人，如果端点本身就是攻击者，那么端点的防护就不可能实现了，这时就需要网络的协助，建立一个严格的准入控制，来判断端点的性质，这种网络协同的准入机制，也就是思科提到的NAC网络存取机制。我们不能说在端点和网络做谁好谁坏，真正好的策略是需要两者的协同的。有些防护需要在网络侧做，比如发现一些server的漏洞，但是终端的应用需求使得不能轻易通过升级终端程序来解决，这时就需要在网络侧部署一些防攻击的手段，将攻击控制在远端。当然，也有很多防护需要在端点做，例如一些针对系统的应用的，如果在网络做，会耗费大量的资源。我们需要通过合理和协同部署，实现网络对端点的识别和判断，并赋予相应的权限。 3、可信安全架构，搭建整体防护堡垒 刚刚我们从具体的细节讨论了如何在网络信息传递过程中做好防护，下面我们从宏观上看一看，如何搭建一个整体的网络防护堡垒。 一个可信的网络安全架构，主要由三个部分组成：可信层、安全层、服务层。 1、可信层：首先保证网络是可信的，各终端接入的是可信的网络，网络也能识别终端是否可以信任。然后提供链路层的加密服务，使得数据在交换机间传输时，可以选择是否采用加密进行保护。最后通过各种组策略，对角色进行权限的控制和管理。 2、安全层：既然网络是可信的，那各个端点间是否要控制呢?当然。我们可以通过防火墙入侵检测，VPN安全网关等，来构建安全层的防护。在安全层中，网络里流转的数据能够被监控、识别、关联和控制管理。例如，在数据中心，不同

场景下我们可以利用防火墙、Email过滤，安全控制，3A认证，VPN等进行隔离和识别和管理，将网络上各个端点各个部分进行管控。 3、服务层：服务层主要由三个功能部分组成。云火墙，实现防止木马.IPS联防，根据IP地址进行协防和联防，发现攻击可以通知其他IP.Email和Web安全，利用SensorBase统一的数据库，即时收集和更新各地的攻击信息，做出防护。 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