采用思科身份服务引擎的规划和部署前检查表

安全访问操作指南系列

作者：Thomas Howard

日期：2012 年 8 月

目录

规划检查表

此检查表旨在作为指南，帮助您了解采用思科®身份服务引擎 (ISE) 成功部署 Cisco TrustSec 所需的各种组件、技术和需要执行的组织工作。将此检查表用于更好地预测重要的集成点，以便随时验证其在您的环境中是否正常运行。

通过回答以下有关组织和运行方面的问题，可帮助您了解一些将影响 TrustSec 在您的网络中进行集成和部署的安全要求、业务流程和组动态。

组织

- 谁是成功部署和运行所需的组织利益相关者？例如：桌面服务、网络工程、网络安全、域管理员、证书管理员、桌面支持等等。
- 这些组是拥有共同的高管愿景，还是只是孤立工作？
- 哪些组负责策略创建和实施？
- 策略决策者更改策略的法定最少人数是多少？

安全策略创建和维护

请描述您需要的网络访问策略。具体包括以下方面的授权和处理：

- 托管用户，包括对不同的组和角色的独特要求
- 非托管用户：访客、承包商、外部网络、实验室等
- 各种网络访问方法的策略，例如有线、无线、VPN 和虚拟桌面
- 不同位置：站点、大楼、楼层等
- 无代理设备：IP 电话、打印机等
- 是根据终端或用户身份、终端状态，还是根据这二者来进行网络访问授权?

规模

- 您的部署总共涵盖多少位置？
- 您期望随时在网络上看到多少并发终端？
- 需要多少 ISE 节点？您的网络中哪些是部署各 ISE 节点的最佳位置？
- 您是否会先采用实验室概念验证 (PoC) 或有限的生产试点来测试所有必要的场景？
- 您是否会先在监控模式下将 TrustSec 部署在您的生产环境中，以便了解情况，然后实施限制？
- 您是否有需要先部署 TrustSec 的高风险区域？
- 对于向整个组织扩大试点，您有何规划？

公共密钥基础设施 (PKI)

- 您是否已部署企业 PKI 或证书颁发机构 (CA)？选择的是哪个供应商？
- 如未部署，您是否期望安装和管理证书或从公共 CA 供应商购买单独的证书？
- 每个服务器证书一年的费用是多少？

- 根据节点的完全限定域名 (FQDN)，每个 ISE 节点都需要一个单独的证书。
- 在贵组织内获取数字证书的流程是怎样的？
- 建议生产部署**不要**采用自签名证书。如果您无法使用公共或企业 CA 签名的证书，贵组织是否完全了解长期可用性、技术支持、迁移和扩展问题？

目录服务

- 您是否会使用用户名和密码或证书来识别用户和设备？
- 您是否会集成 Microsoft Active Directory 之类的现有身份库？轻量级目录访问协议 (LDAP)？RSA SecurID 令牌？
- 您是否有多个身份域或林要进行身份验证？有多少？
- 您现有的身份库集群是否会扩展至支持来自网络身份验证的负载？

网络接入设备 (NAD)

- 您想要使用 ISE 对您的网络的哪些边缘进行身份验证？有线？无线？VPN？
- 相关 NAD 是否具备适用于 TrustSec 解决方案的推荐软件？有关最新推荐网络设备及相应软件版本的信息，请参阅 http://cisco.com/go/trustsec。
- 您的现有硬件是否支持推荐的软件版本和所需的 TrustSec 功能？

托管终端

- 您是否知道您的网络上目前存在多少托管网络终端？
- 您是否已在使用思科或 Microsoft 提供的 802.1X 请求方？是有线或无线，还是二者都用？
- 所需的 802.1X 请求方是否要求购买软件、升级或操作系统服务包?
- 需要或首选哪些身份验证类型？
- 要使终端兼容，需要什么额外的安全软件？
- 对于所有需要的终端，您是否有足够的安全软件许可证（AV、HIPS 等）？

无代理终端

- 您是否有办法在您的网络上自动识别无代理终端并为其授权？
- 您是否已确定您的网络上无代理设备的总数及设备类型？

1. 无 802.1X 请求方（其操作系统不支持或已固化，例如电话或打印机）
2. 预执行环境 (PXE) 网络引导和重新映像
3. 其他非托管/不可控的设备（访客、实验室等等）

- 您用什么方法来确定无代理终端、对其分类并为其授权？

1. 在硬件和/或操作系统中升级至 802.1X 功能
2. 使用 MAC 身份验证绕行 (MAB) 在 ISE 中制作白名单

- 手动 MAB 或终端注册系统的预期运行成本是多少？

思科身份服务引擎 (ISE)

- 您是否需要从现有的访问控制系统 (ACS) 或网络许可控制 (NAC) 设备部署进行迁移？
- 您需要根据贵组织的规模、网络可用性要求、重新验证频率和协议选择，扩展部署多少 ISE 节点？有关如何执行此方面计算的信息，请查阅《TrustSec 设计和实施指南》。
- 处理大量并发授权是否需要任何负载均衡硬件或软件？

访客服务

- 对于无法通过 802.1X 或 MAB 进行身份验证的访客、访问者甚至员工，您采取什么安全策略？
- 您是否需要从现有的访客门户（例如思科 NAC 访客服务器）进行迁移？
- 允许何人发起访客帐户？前台员工、所有员工或自行注册？
- 您将允许发起人调配哪些不同的访客服务配置文件？使用日期时间还是从首次登录起的时间？
- 您将要求访客提供什么信息来获得网络访问权限？
- 您将如何审核发起人、调配的帐户和帐户使用情况？

监控、报告和故障排除

- 您现在使用什么监控和报告应用或工具集？
- 对于所有这些新日志和事件，有什么长期存储要求？

通信

最好的做法是，在您的网络访问策略中清楚地传达变更，从而使不合规用户不至于对新的安全和软件要求、访问限制或 URL 重定向感到意外。

- 您是否从管理层获得了明确授权来阻止、限制和重定向不合规终端和用户？
- 您是否已经提高所有利益相关者和用户对于此网络访问权限变更的认识（需求、好处）？
- 负责的小组是否已准备好统一回应不合规用户？
- 是否将通过多种渠道，包括邮件、内联网、补救站点和支持部门，传达这些网络安全变更？

支持部门

- 支持人员是否就新的安全技术、流程和策略接受了培训？
- 支持人员如何对基于 ISE 的 RADIUS 身份验证相关支持来电进行故障排除？
- 是否需要为 ISE 相关支持开发任何内部工具或应用？

部署检查表

请根据您对规划检查表中问题的回答，以及您的现有网络架构，填写以下部署检查表表单。这些表将为现场工程师提供宝贵的参考，加速思科 ISE 和网络设备的初始配置。

安全策略

描述您的主要网络访问场景，以及您将如何使用基于情景和网络的属性来实施安全访问。考虑各种场景，例如用户与终端身份验证、托管终端状态、非托管终端识别、基于角色的识别和分段（员工、承包商、访客等）或基于位置的区分。这些独特的授权状态将直接映射至您的最终 ISE 授权规则和策略。

表 1. 安全策略

场景	用户组	终端	情况（位置、网络访问 - 有线/无线、时间、身份验证协议等）	授权状态
使用企业设备的员工	域用户	域计算机	认证协议 = 扩展认证协议传输层安全性 (EAP-TLS)	员工访问权限
使用个人设备的员工	域用户	iPad、Android 或 iPhone		

实施状态

根据您在表 1 中指定的唯一授权状态，在表 2 中记录针对每个状态的具体 RADIUS 属性设置。这将有助于您了解每个实施状态之间的细微差异并确定您必须创建的唯一 ACL 的数量。

表 2. 授权配置文件

RADIUS 属性	授权配置文件	
	员工访问权限	有限访问权限
VLAN ID/名称	接入	接入
重定向 URL	-	-
URL 重定向 ACL	-	-
可下载的 ACL 名称	ACL - 全部允许	ACL - 限制
语音 VLAN 权限	否	否
重新身份验证：计时器	28800（8 小时）	28800
重新身份验证：保持连接	是	是

数字证书

创建并使用 CA 为您的 TrustSec 基础设施签发的证书，最大程度地减少由于不受信任、自签名证书导致的长期问题（表 3）。

表 3. 要申请的数字证书

组件	FQDN	组织单位	组织	城市	省/自治区	国家/地区（2 个字母）	最大密钥长度	证书格式
证书颁发机构								
ISE Admin #1								
ISE Admin #2								
ISE PSN #1								
ISE PSN #2								

网络服务

记录所有基本网络服务以及在您的网络中提供这些服务的主机（表 4）。这将帮助您创建访问控制列表 (ACL) 异常和 TrustSec 服务配置。

表 4. 基本网络服务列表

角色	DNS 名称	网络地址	协议	详细信息
CA 服务器				
DNS 服务器			UDP:53	
DHCP 服务器				
NTP 服务器			UDP:123	
FTP 服务器			TCP:21	username:password
代理服务器（至互联网）			HTTP/S:#	username:password
TFTP/PXE 引导服务器			UDP:69	username:password
系统日志服务器			UDP:514	username:password
身份库：Active Directory				username:password
身份库：LDAP				
身份库：OTP				
ISE 管理员节点			HTTP (TCP:80) HTTPS (TCP:443)	CLI: admin: cisco Web: admin: cisco RADIUS Key:
ISE 策略服务节点			HTTP (TCP:80) HTTPS (TCP:443) RADIUS (UDP:1812) RADIUS (UDP:1813) CoA: 1700 & 3799	CLI: admin: cisco Web: admin: cisco RADIUS Key:

终端

在表 5 中，指定启用 TrustSec 时各种网络终端如何进行身份验证。可能的身份验证方法包括 802.1X、MAB 和 Web 身份验证。

表 5. 终端详细信息

终端	身份验证方法	注
Windows XP SP#（本机请求方）		
Windows Vista SP#（本机请求方）		
Windows 7（本机请求方）		
Windows 7 (AnyConnect®)		
Windows XP SP3		
Apple Mac OS X 10.7.x（本机请求方）		
Linux		
Apple iOS 设备		
Android 设备		
思科统一 IP 电话 7900 系列		
思科接入点		
打印机		
服务器		
访客		
PXE 引导		

网络设备

使用表 6，按照型号、主管（如适用）和软件版本记录您的网络中每个类型的网络接入设备。我们强烈建议您将所有交换机升级至经过测试和验证的最新 TrustSec 版本，以免功能和行为不一致。除非您使用通配符条目，否则必须将每个网络设备 IP 地址添加至 ISE 中。

表 6. 网络设备列表

型号	Cisco IOS® 软件版本	管理 IP 地址	管理 DNS 名称

测试场景

大规模部署之前，请根据您所需的安全策略、预期的终端和实施状态，创建一个场景列表，在实验室或小型概念验证部署中进行测试。表 7 列出了一些建议的入门场景。

表 7. 测试场景

场景	结果（通过/失败）	备注
设备分析		
MAB		
Windows 计算机身份验证		
对 Active Directory 域进行用户身份验证		
单点登录 (SSO)：用户名/密码		
访客发起		
访客访问权限		

附录 A：参考

Cisco TrustSec 系统：

http://www.cisco.com/go/trustsec
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

对于 Cisco Catalyst 2900 系列交换机：
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000 系列交换机：
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000-X 系列交换机：
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 4500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 6500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

对于 Cisco ASR 1000 系列路由器：
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html