概览

Cisco® Identity Services Engine(思科身份服务引擎)

管理并保护移动企业

企业网络早已告别依靠四壁围挡来保护安全的时代，现已延伸到员工和数据所及的任何地方。如今，员工需要用空前多的设备，通过更多的非企业网络来访问工作资源。移动性和物联网（IoE）正在改变我们的生活和工作方式。企业必须能够支持大量新型网络设备。然而，无数安全威胁以及高度公开化的泄密事件表明，确保安全访问不断演进的企业网络至关重要。

随着现代网络的扩展，调度资源、管理全然不同的安全解决方案以及控制风险所面临的复杂性也在与日俱增。在 IT 资源本已捉襟见肘的情况下，“物联网”的迅猛增长以及无法识别和修复安全威胁的潜在影响，已经成为真正巨大的挑战。

不断演进的移动企业确实需要采取与以往完全不同的方法才能进行管理并确保安全。这种全新的方法称为Cisco® Identity Services Engine（思科身份服务引擎， ISE）。

减少漏洞并降低风险

为实现上述目标，必须深入了解访问企业网络的用户和设备，并采取适当控制，从而确保仅有正确的用户通过正确的设备才能获得正确的企业服务。

无论有线和无线访问多厂商网络，还是远程VPN连接，经过重新设计的ISE 2.0简化并统一了高度安全的访问控制。思科ISE凭借其智能传感器和卓越的分析能力，深入网络内部，提供正在访问资源的人与物的高度可视性。

通过与生态系统合作伙伴的集成软件分享重要的场景数据，以及实现Cisco TrustSec®软件定义细分策略，ISE将网络从单纯的数据管道转变为安全性的执法者，缩短了对于网络安全威胁的检测时间和修复时间。

优势

- 集中并统一高度安全的访问控制，无论终端用户是通过有线还是无线网络或VPN连网，均可以业务角色为基础，为其提供始终如一的网络访问策略。
- 通过Cisco® Identity Services Engine（思科身份服务引擎 ISE）卓越的设备分析与设备特征更新服务，获得更高的可见性与更精确的设备标识，从而减少未知终端的数量。
- 提升访客体验，通过完全可定制的品牌化移动和桌面访客门户，更加轻松地实现访客接入和管理，通过动态可视化工作流程数分钟即可完成门户创建，从而轻松地对访客访问进行全面管理。

- 通过开箱即用的轻松设置、自助设备连接和管理、内部设备证书管理和集成的企业移动性管理 (EMM) 合作伙伴软件来管理公司自有和外带设备连接，加快实现自带设备（ BYOD ）和企业移动性。
- 通过使用Cisco TrustSec®技术来构建软件定义的细分策略，涵盖网络安全威胁方面的考虑，以便加强路由和交换层的基于角色的访问控制。这样可以在避免多VLAN复杂性及无需网络重构的情况下，对访问权限进行动态细分。
- 与合作伙伴的网络和安全解决方案共享场景数据，提高其效率并缩短其对于网络安全威胁的检测时间（TTD）和修复时间（TTR）。
- 通过与思科Firepower管理中心的整合，ISE可以缓解受感染的终端，并且进行修复，观察和清除。

ISE 2.0的更新和增强功能包括：

- 与思科移动服务引擎集成提供位置数据。企业可以创建并进行与特定位置相关的访问，例如，医疗专业人员仅限在急诊室内访问病人的医疗记录。
- 为特定的ISE生态系统合作伙伴增强我们的开放式体系结构，使客户可以采用其现有的安全解决方案与ISE协作，识别网络威胁，迅速遏制并修复。
- 支持第三方网络接入设备（NAD）和IPv6终端，ISE可以终端可以通过更多的网络设备，合规的进行访问。
- 精简策略管理，包括以TACACS +简化设备管理，简化有线接入功能，从而更为轻松地为有线网络部署高度安全的访问控制策略。
- 伴随思科AnyConnect® 4.2而来的是新型网络可视性模块。在以前自带终端无法获得的应用程序流量方面，该组件可以提供一定程度的详细信息。

此外，ISE使用思科平台交换网（pxGrid）技术与集成的生态系统合作伙伴解决方案共享丰富的场景数据。这一技术增强了其识别、减轻和修复遍布企业扩展网络的安全威胁的能力。总之，访问控制得到了集中和简化，可以安全地提供关键业务服务、增强基础设施安全性，实施合规性策略并简化服务运营。

通过与领先的安全信息和事件管理（SIEM）及威胁防御解决方案的集成、其深入的网络可视性和访问控制能力，ISE在Cisco Cyber Threat Defense（思科网络威胁防御）、思科“网络作为传感器”（Cisco as a sensor）和思科“网络作为实施者”(Cisco as an enforcer)解决方案中起着不可或缺的作用。最终，ISE提供了企业所需的可视性、场景信息和动态控制，以便帮助其切实落实整个攻击发生过程中的安全目标：在攻击发生之前管理网络；在攻击发生期间提供可见性并遏制威胁；在攻击发生之后缩短检测时间（TTD）及修复时间（TTR）。

C45-654884-13 10/15