白皮书

从远程访问到安全移动：实现新一代的员工工作效率

为什么移动性很重要

技术不断为提高工作效率带来新的机遇。能够接受并利用技术创新（尤其颠覆性创新）的企业通常能够在市场中获胜，或者能够比不接受创新的企业占有更多市场份额。如今，新一轮技术冲击效应正在来临：企业移动性高度扩展，员工可以随时随地开展工作。

对企业而言，企业移动性并不陌生。事实上，远程访问和远程办公解决方案已经存在很长时间了。但不同于以往的是，企业需要有能力支持企业移动平台惊人的变化速度，而这种变化是由员工而非传统的 IT 团队引起的。

要保持竞争力并转变为一种新型高效工作负载模式，企业必须考虑接受移动性。在当前的经济困难时期，裁员和全球外包已经成为常态；企业必须用较少的资源来做更多的事情。接受移动性最符合企业组织的利益，因为与我们使用互联网所带来的益处相比，它更能提高工作效率。

移动性不仅是竞争上的必要举措，也是当今高度变化的员工的迫切要求。未来 20 年，随着婴儿潮时期出生的人逐渐退休，这一代人在就业人口中所占的比重会越来越小；从全球范围来看，80 后至 00 后将迅速发展壮大，赶上或超过 50 后的就业人口。年轻一代都依赖于社交网络、互联网社区、持续沟通和信息交流。现在，许多年轻人生长在这样一个互联网连接无所不在的时代，利用他们“始终在线”的能力，可能会大幅提高工作效率。

接受移动性面临的挑战

很多企业花费数百万美元的巨资来建立网络和安全基础设施，并在边界谨慎寻找开口，提供远程访问连接。事实上，在笔记本电脑发展成为首选移动设备的过程中，VPN 发挥了重要作用。然而，这种情况正在迅速改变。仅仅几年前，智能手机和平板电脑就超越了传统基于 PC 的设备的计算能力，它们的用户界面更丰富、设计更精良，可作为语音通信设备，内置对无处不在的无线连接的支持，这些优势使得它们迅速成为员工的首选设备。

企业可能面临的最大的挑战是失去控制。在这种新的形势下，消费者（同时也是企业员工）正在推动这场变革。他们把钱花在界面更流畅、用户体验更好且更加便捷的设备上。员工正寻求通过各种方式在企业网络上使用这些设备（无论准许与否），与此同时，用于阻止此类使用的企业标准很快就被规避掉。

变化的速度对企业也是一项挑战。企业 IT 团队必须快速适应一系列的新型移动平台；他们必须重新评估与新设备相关的安全态势和框架。消费者采用新技术的速度比制定标准的速度更快，而旨在帮助管理大量要求支持这些全新移动设备的请求的工具也在逐渐落伍。

而最基本的挑战或许在确保新访问模式的安全方面。从根本上来说，旧的安全模式“外强中干”，不再适用于当今的移动性环境。外围边界真正消失了，网络边界无处不在，有时甚至就在移动员工手中。失去这些移动设备，会对企业造成哪些不利？而它们会通过何种方式将传统安全威胁带入网络？企业可能配置了用于处理一些设备（例如 PC）的此类问题的基础设施，而对于另一些更新形式的设备，企业则可能缺乏保护企业数据、确保网络安全以及为应用访问提供足够的服务级别的能力。

© 2011 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

答案：安全移动

企业及其 IT 团队需要一个框架和各种解决方案来实现安全移动性。思科认为解决此类问题的方法是采用可提供访问权限、安全功能和选择余地的安全移动性：

- 轻松**访问**用户完成工作所需的应用和信息
- 可保护终端不受威胁、对设备实施公司策略的精确**安全性**
- 能支持各种设备，以便用户能够**选择**要使用的工具

这些基本特征为企业奠定了接受移动性所需的基础。

思科的价值主张

思科迎来了安全移动，呈现了一种思科活动的任何相关人员都可“随时随地”实现优化连接的网络态势。Cisco® AnyConnect 安全移动解决方案在这种框架中用作可无缝安全地实现移动员工的一系列解决方案。AnyConnect 解决方案包括 Cisco ASA 系列设备、Cisco AnyConnect 安全移动客户端、网络安全增强功能以及 Cisco IronPort 网络安全设备或 Cisco ScanSafe。

AnyConnect 安全移动解决方案

Cisco AnyConnect 客户端是一个统一的终端软件客户端，与当前所有主要企业移动平台（PC 和小型设备）兼容。AnyConnect 安全移动解决方案基于基本 VPN 技术，将其价值主张延伸到了远程访问以外，提供一流的用户友好体验和基于网络的出色安全性。在终端计算机设备上，AnyConnect 安全移动功能可在防火墙后面的网络结构中实现安全性，并且当用户在防火墙以外移动时，可提供前所未有的安全性和企业策略支持。

下面一节将详细讨论企业在实现移动性过程中所面临的安全挑战，以及 AnyConnect 安全移动解决方案如何帮助弥合安全移动的现实与期望之间的鸿沟。

企业实现移动性所面临的障碍

VPN 打开 - 尽管能够为移动工作人员带来灵活性，但 VPN 同时被认为是当今企业最大的安全漏洞之一。企业在加强互联网边界外围方面花费大量资金后，仍没有认识到笔记本电脑现在已经构成该边界的一部分。当互联网活动通过企业网络引导时，其他网络代理技术可以拦截不良站点。目前市场上的大多数 VPN 客户端对最终用户而言都是很繁琐的，往往需要重复启动会话。由于此原因以及带宽方面的考虑，致使最终用户在互联网上自由漫游而不启动 VPN。未受保护的互联网冲浪导致分离隧道起作用，让恶意软件有机会使终端感染病毒，然后一旦允许终端返回，终端自身会在企业网络中传播病毒。

Cisco AnyConnect 安全移动解决方案有助于补救传统 VPN 的这一漏洞。2010 年，思科成为针对 PC（Windows、Mac 和 Linux）引入跨平台解决方案的首家供应商，该解决方案包括可配置的持续性 VPN 以及集成网络安全。在“始终开启”模式下运行时，AnyConnect 解决方案可保持使用方式的一致性，并能通过思科 IronPort® 网络安全设备推动实施安全策略。Cisco AnyConnect 客户端身份验证凭证将应用特定的网络使用策略和安全措施，这些策略和措施可以因用户连接发起位置（企业实际外围内部或外部）的不同而异。

“黑暗网络” - 鉴于网站域名的爆炸性增长，大部分的互联网仍未进行分类。目前，大部分的 PC 终端病毒感染是通过恶意网站传播的。关联性或主动扫描能够用于对属于“黑暗网络”的 IP 地址进行更准确地分类。思科使用其业内领先的网站信誉过滤和动态分类技术了解这些网站。随着时间的推移，思科的安全智慧操作 (SIO) 中心对通过思科大部分的安全设备和产品获取的 IP 信息制定了全球关联性。

端口 80 门户 - 尽管多年来认为即时通讯等基于 TCP 的应用是终端安全感染的充分理由，但这个问题只是愈演愈烈。随着当前的 Web 2.0 应用建立了新水平的快速通信和社交互动，恶意链接和安全威胁的可能性比以往任何时候都要高。

© 2011 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

AnyConnect 安全移动解决方案能够确保对所有经过端口 80 的终端设备流量都进行深度的恶意内容检测。此外，可应用基于用户或团队身份的一致性安全策略，从而能够允许或拒绝对特定 Web 应用的访问。

SaaS 泄露 - 将企业应用迁移到内部数据中心之外，是加快移动性发展步伐的另一个附属趋势。如果设备可通过互联网连接，并且支持浏览器访问，则可以访问位于网络上的应用程序。在这一背景趋势下，企业数据越来越多地保存在托管软件即服务 (SaaS) 企业应用的公共互联网网站的后面。IT 团队甚至有可能不知道 SaaS 应用在其企业客户群中的利用程度。即使对于允许使用和支持的 SaaS 应用，监控和管理访问这些分散应用所需具备的技能都足以令人却步。AnyConnect 安全移动解决方案使用安全声明标记语言 (SAML) 为 SaaS 应用创建单点验证、撤销和管理。对于支持的应用，最终用户无需记住其他密码，如果其 IT 团队未禁用访问，即可无缝进入关键 SaaS 应用。

设备丢失 - 智能手机或平板电脑丢失或被盗对其所有者可能是灾难性的，会导致金钱损失、个人和公司信息丢失，以及丧失工作效率。但是，对企业而言，业务挑战和潜在法律后果还要糟糕得多。设备丢失后，设备上存储的敏感信息有可能被滥用，而且设备有可能被用来访问关键业务系统，这些情况会迫使企业花费上数千元（即使不用数百万元）来处理突出事件响应、信息与系统恢复以及负责披露成本。

为了在移动设备丢失时提供一级保护，必须对所有访问企业信息的移动用户实施全面的设备安全措施。Cisco AnyConnect 安全移动解决方案支持使用数字证书，当设备丢失时，可立即撤销该证书，拒绝其访问网络。PIN 锁定、设备加密以及非“越狱”手机等策略即使在设备丢失的情况下也可以确保设备安全，将减少由于移动操作系统平台被打开而引入的威胁。每个组织必须确定它们需要哪些智能手机和平板电脑策略，同时必须配合每个平台的功能实施相关级别的安全性。很多企业会发现有 Exchange ActiveSync 就已经足够了，但有些企业则需要移动设备管理解决方案的高级功能来补充和加强 AnyConnect 的内置安全功能。

IT 消费化 - 企业过去往往指定员工所使用 IT 设备的类型。这样，IT 可以对设备和终端保持控制权，从而确保实施一致的安全措施。IT 正在转向一种由员工购买其自己的移动设备或 IT 对购买设备进行报销的模式。无论哪种方式，员工都可以选择他们要在企业网络上使用的设备。这种员工灵活性和自由选择的代价是，IT 再也无法指定每个设备上将显示什么图像，因为每个设备都是个人的自有设备。

AnyConnect 安全移动解决方案可通过在每个终端上使用 AnyConnect 客户端来解决这一问题。对笔记本电脑、智能手机和平板电脑等众多设备的支持意味着，可以轻松实施并始终保持基本的安全连接。此外，思科网络安全设备或 ScanSafe 中的基础网络安全能够确保一致的策略实施，无论用户是在办公室还是远程访问信息。

总结

企业不应反对 IT 消费化和新的移动设备、连接和应用潮流趋势，而应将移动环境视为一种可提高员工与合作伙伴工作效率和创造性的全新模式。移动性已经成为既定事实，IT 部门需要找到一种方式在他们的移动设备上统一实施安全措施。

使用 Cisco AnyConnect 安全移动解决方案，企业能够接受移动性，并利用其现有的基础设施和流程来提供随时随地从任何设备的安全访问。

要了解 Cisco AnyConnect 安全移动客户端，请访问 http://www.cisco.com/en/US/netsol/ns1049/index.html

© 2011 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

美洲总部
Cisco Systems,Inc.
加州圣荷西

亚太总部
Cisco Systems(USA)Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

Cisco 在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。

Cisco 和 Cisco 徽标是 Cisco Systems, Inc. 和/或其附属公司在美国及其他国家/地区的商标。在 www.cisco.com/go/trademarks 上可查看思科商标列表。提及的第三方商标为其相应所有者的财产。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1005R)

美国印刷 C11-641140-01 04/11

© 2011 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。