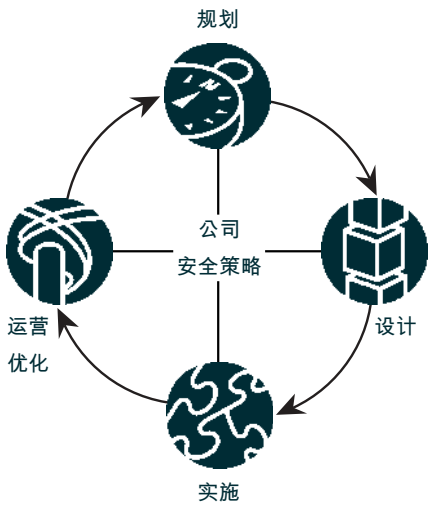
思科网络安全高级服务

思科网络安全高级服务



对企业而言，保证网络基础设施安全从未象现在这样严峻和重要。为确保企业的安全运营，安全必须真正成为网络的一部分，部署在您的整个环境中，以保证网络安全不受威胁。

为解决这些问题，思科网络安全高级服务提供了专家级的指导，帮助您免于网络安全威胁所带来的影响，使机构的工作效率和总体拥有成本（TCO）都达到预期的目标。思科系统公司的独道之处在于它所提供的全面综合的服务，其中安全是网络必不可少的内容。

思科高级服务团队由网络安全领域的专家组成，这些专家曾负责过许多全球财富 500 家公司的安全运营。另外，思科高级服务顾问都持有专家级的 CCIE 和 CISSP 证书，并在规划、设计、实施和优化大型网络安全基础设施方面拥有丰富经验。

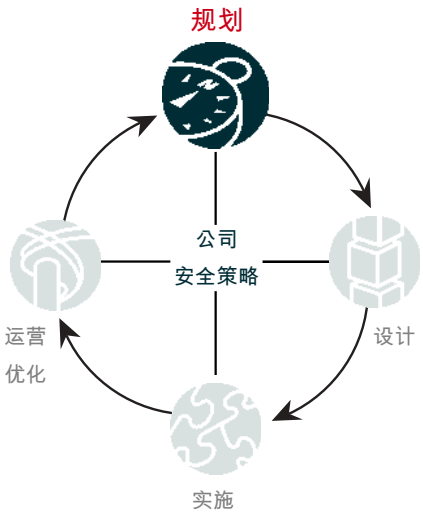
凭借实际的经验，对最新网络安全技术的全面洞察，以及专业化的工具，思科高级服务设计团队可以深入地了解您的商业目标和安全环境，帮助您对愈演愈烈的信息安全威胁进行管理。

当您与全球的大型公司开展业务合作，尤其是将基于互联网的系统与网络连接时，安全和可靠性就成为一个关键问题。这时，思科是您的轻松选择。如果您想成为一家像我们一样，从基础设施，公司声誉以及产品都基于一个拥有互联功能，健全和功能强大的网络时，与业界领先的公司携手共进无疑是一种明智的选择。

—— FuelQuest 公司副总裁兼首席执行官 Kirt A.Scott

支持网络周期的安全服务

思科网络安全高级服务可以在网络的整个使用周期中提供安全服务。思科专业技术人员为满足您的公司安全策略要求提供了专家级的建议，可以帮助您成功地规划、设计和管理您网络基础设施中基于网络和基于主机的入侵检测传感器、防火墙设备和 IP 安全（IPSec）VPN 等安全技术的集成。



规划：网络安全评估和规划

思科的网络安全评估和规划服务的范围，从开发公司的安全运营策略，到网络化应用、系统和设备的安全评估，无所不包。通过对网络化的商务环境进行全方位评估，思科可以帮助您针对网络入侵的检测，防卫以及响应能力进行审定。

安全状况评估

作为规划网络安全的第一步骤，思科为您提供公司网络安全状况的综合评估报告。安全状况评估（SPA）通过执行一项关于公司网络设备、服务器、桌面和数据库的全面评估，为您的网络安全状态提供了一份简报。参照业界公认的最佳方案，思科专家对您的网络安全有效性进行分析，从而使您对自身安全的优势和不足有所认知，并对可能威胁您业务的特定安全漏洞作出文档报告。

由于网络安全涉及业务的各个层面，思科工程技术人员将从各个角度对安全进行评估，包括您的内部、外部、拨号和无线网络，并为您改进总体网络安全提供建议。思科具备丰富现场经验的安全专家，将利用专业化的工具进行综合研究，并对可能造成的网络系统和信息的未经授权入侵访问的安全漏洞加以标识（表 1）。

内部评估

对远程黑客滥用互联网所造成的威胁和突发事件我们十分关注，但由此却可能忽视了内部可信赖网络的安全。内部评估是一种可控的网络攻击模拟模式，用于检测内部系统、应用和网络设备的表现状况。评估针对反击蓄意性攻击和应付内部可信赖员工的非蓄意性错误所需采取的步骤进行了确认，以便更好地保护有价值的信息资产。

针对非授权访问内部资源，内部SPA评估采取了一种综合手段，除了自动漏洞检测外，思科专业技术人员还利用一种可控、安全的模式对入侵行为进行真实的模拟，并进行手工安全漏洞的确认，这种更富于结构化的方式，可使通过自动方法未检测出的漏洞得以及时发现，这种二次检索可检查出包括试图利用主机间的信赖关系，利用口令的弱点，或获得系统的管理访问权等活动。

外部评估

外部评估旨在对与互联网连接的有关系统的安全风险进行定量分析。为了有效地识别在允许外部非信赖网络接入内部可信赖网络和系统的过程中所存在的漏洞，思科专业技术人员对恶意攻击者试图损害周边设备和互联网安全控制能力等典型敌对行为进行了模拟。

首先，思科专业技术人员利用功能远超出标准商业工具的专业自动化工具，对公司在互联网上的状况进行远程漏洞扫描，在对互联网设备注册作出研究和确认之后，思科专家会针对外部网络可见的服务进行扫描。因为大多数服务都存在固有的、众所周知的漏洞，思科专业技术人员对所提供服务的潜在漏洞予以搜索，并对可能造成安全损害的漏洞予以人工确认。

无线评估

为识别与无线部署有关的安全风险和暴露情况，无线评估为公司无线网络提供安全状况评估。思科专家对用于识别授权和未授权接入访问点的无线技术网络结构和配置进行分析，并推荐了解决方案以强化无线基础设施的安全。

首先，思科专家对客户现场进行调查，以发现和记录所有可能的接入点。通过将站点调查收集的数据与授权设备列表进行比较，使思科得以识别可能的入侵设备。在接入点调查完成后，思科专业技术人员将无线网络结构和配置与业内最佳方案进行比较，从而列举出已知的漏洞和威胁。

在客户的建筑物外，技术人员采用先进的无线天线技术，找寻建筑物的无线网信息漏洞。必要时，技术人员将进入建筑物的控制中心继续追踪无线LAN信息。在信息发现后，技术人员会确定所使用的加密和验证级别，寻找可能被用于接入LAN的网络属性，如网络地址。

拨号评估

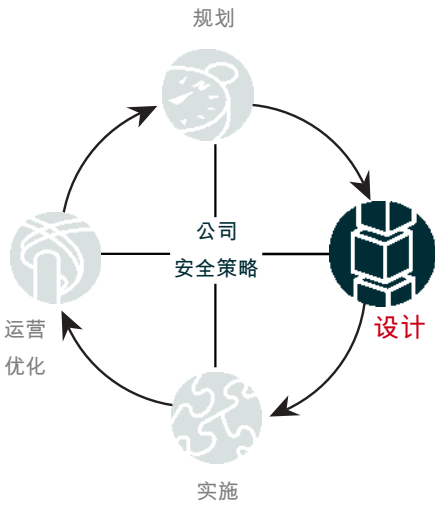
拨号评估旨在确认与远程服务有关的安全风险。拨号服务可为攻击者入侵客户网络大开后门，使其得以穿过原本有效的安全措施，例如防火墙。在确认了服务器软件和验证方式之后，思科专业技术人员将尝试未授权访问远程接入服务器。技术人员将以手工尝试绕行接入服务器。从而确认受损害设备与网络的连接点，可能的话，再进一步尝试接入。

安全状态评估分析和报告

思科专业技术人员提供了深入而详尽的模拟攻击分析报告，包括对公司网络状况量化的管理参数和图表。SPA 报告还提供了深入的技术分析，包括各个 IP 地址分析，解释用于损害网络系统和设备的手段，以及攻击者采用同一攻击手段的可能性说明。然后，对已发现的漏洞进行优先级排序，为纠正安全风险提供措施建议，并对防范未来入侵所采用的补救措施予以详细说明。

表 1 安全状况评估的特性与优势

功能与措施	优势
功能 • 内部评估 —对端口进行自动扫描，以确认潜在的漏洞 —模拟可控网络攻击，从而评估系统应用程序和网络设备的漏洞 —执行二次检索，确认已识别的漏洞 • 外部评估 —公司有关互联网设备作远程扫描 —对试图损害周边设备的敌对行为进行模拟 —详细分析对设备、服务器和信息的未授权访问 • 拨号评估 —尝试获得远程接入服务器的未授权访问 —确定所使用的验证方法，并试图人为绕开它 • 无线评估 —确认可能构成安全隐患的无线网接入点 —提供风险分析和网络内暴露点的研究 —提供配置调整建议，最大限度地降低风险 **措施** • 目标网络设备、系统和服务的基线测试 • 外部接入测试、远程调查和在线内部模拟攻击，用于发现漏洞 • 数据与智能分析相结合，对设备、系统和信息的安全威胁情况予以评估 **内容**———一份 SPA 管理和技术报告，包括漏洞分析，归档并按漏洞的严重级别进行排序，以及补救建议；并在客户现场作一次关于已发现的漏洞和补救措施的讲座	**消除网络安全威胁因素** • 提供经济有效，无倾向性的信息安全风险评估 • 确定给网络、系统和信息带来风险的主要安全威胁 • 支持公司对现有安全策略和过程的有效性进行评估的要求 • 为消除已识别漏洞提供建议，从而为改进网络安全状态提供支持



设计：构建可扩展、适应性强，使用方便的安全解决方案

在完成对网络安全状态评估之后，思科可与您携手共同开发一个强大的网络安全设计方案。思科的设计方案对网络安全及其与核心网络基础设施的集成进行了全方位的周密思考。借助一种基于业界标准，广泛而深入的研究模式，思科专家将帮助您开发一种多层防御体系，以抵御黑客的直接攻击，或来自病毒和蠕虫的非区分性攻击。

思科设计支持使您得以为客户提供当前所需的安全应用服务，因而强化了您在竞争中的地位。借助架构式设计方案，我们的安全基础设施不仅可以满足当前的需要，还可以随着时代的发展不断更新，为全新商务应用的部署提供支持。

通过在公司中部署可重复的安全解决方案、策略和实践的通用集合，思科帮助您节省了网络安全管理的时间和资本投入，降低了网络的总拥有成本，从而达到了降低网络运营成本的目的。

网络安全设计审核

无论从运营还是技术的角度，思科都可以与您携手共建一个强大的安全设计方案。思科安全顾问可以为您在确定作为安全电子商务基石的策略、标准和流程的过程中提供支持，并可与您共同开发安全架构和设计，以支持公司的安全策略。

思科网络安全设计师将对公司的商务策略和相应的安全目标、要求和标准展开协作评估。然后，由思科专业技术人员提供一份有关网络安全架构的深层次的分析报告，以确定其是否能够满足企业和IT策略的要求。根据收集到的网络信息的结果分析，思科专业技术人员提供一份详尽的网络漏洞研究报告。

在对现有网络漏洞评估完成之后，思科专业技术人员将为网络解决方案的安全需求提供建议和优先级排序，包括入侵检测、远程接入、主机保护、周边控制和VPN。思科还可以就如何改进网络设计提供建议，包括网络拓扑结构、设备安置和连接等。在对网络安全的各个层面，如可扩展性、性能和可管理性进行全方位考虑之后，思科可以根据安全部件分别提供协议，策略和特性改进建议。

表 2 网络安全设计审核的特性与优势

功能与措施	优势
功能 ● 审核网络安全商业目标、对象和要求 ● 审核现有网络安全架构和设计 ● 架构和设计漏洞的确认与分析 ● 提供有关网络安全部件的详尽分析，部件包括： —周边设备 —远程接入设备 —入侵检测系统 —防火墙 —路由器和交换机 —外部网连接 —安全管理系统 ● 为拓扑结构、部件功能和特性改进提供建议 ● 为防火墙、入侵检测系统、路由器、交换机、VPN、接入控制服务器、无线设备和安全管理工具开发样本配置 ● 确定软、硬件需求，包括网络安全管理工具 ● 为安全解决方案的持续管理和维护提供建议 **措施** ● 利用设计讨论会收集数据和启动设计审核 ● 针对公司策略和要求，分析现有网络安全架构 ● 参照业界最佳实践，提供初始和最终的差距分析报告 ● 为网络基础设施的全新安全需求提供影响分析 **所提供内容**——网络安全设计审核，用于确认现在网络的漏洞；为总体安全设计部件和功能提供改进建议；提供网络图解和配置样本	**消除网络安全威胁因素** ● 确认安全漏洞，根据公司安全策略和业界最佳方案予以调整 ● 帮助提高网络安全的有效性，提供多层防御体系以抵御安全威胁 ● 改进网络安全设计的可靠性、可维护性和性能 **提高工作效率** ● 缩短了成本既高又耗时的网络设计所需时间 **降低总拥有成本** ● 采用网络基础设施的现有安全功能 ● 通过确保安全策略的持续部署，降低了运营成本，最大限度地缩短了网络中断时间

网络安全设计开发

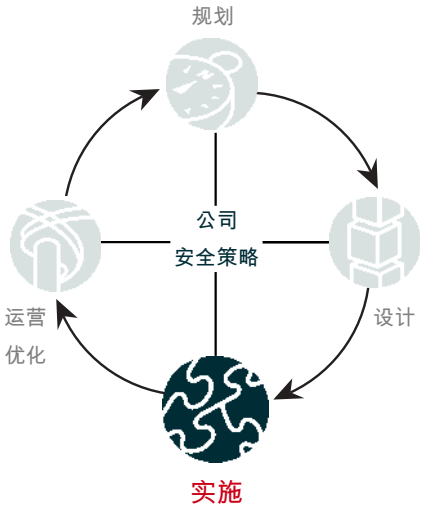
网络安全设计开发服务为将全新安全解决方案集成入核心网络基础设施，提供了开发策略、规划和设计方面的支持。思科顾问和设计师在充分了解公司的安全目标之后，将针对定制的安全部署提供深层次的技术、流程和资源需求分析，以满足公司的安全要求。

借助这一服务，思科专家可以帮助您将与部署全新安全解决方案相关的错误降至最低限度，通过采用思科在一系列网络安全技术，包括入侵检测、防火墙、远程接入和 VPN 等方面的丰富经验，公司将能避免潜在的代价高昂的错误或延迟。

在充分了解您的安全解决方案的目标与要求后，思科专家将帮助公司开发针对安全解决方案的策略和设计，包括详尽的网络图解和配置样本，以便轻松地集成入公司环境。

表 3 网络安全设计开发的特性与优势

功能与措施	优势
功能 • 分析网络安全解决方案的目标、对象和要求 • 联合开发公司网络安全策略、规划和设计方案 • 评估现有网络架构，确认架构、设计和实施的漏洞 • 优化解决方案设计，提高可扩展性、冗余性和性能 • 联合开发一项详尽的设计方案，包括网络安全部件的配置样本，部件包括： —周边设备 —远程接入设备 —入侵检测系统 —防火墙 —路由器和交换机 —外部网连接 —安全管理系统 • 为网络安全协议、策略和特性提供详尽的网络图解和样本配置 • 确定软、硬件需求，包括网络安全管理工具 • 为安全解决方案的持续管理和维护提供建议 **措施** • 利用设计讨论会收集数据和启动安全设计的开发 • 针对公司策略和要求，分析现有网络安全架构 • 开发网络安全策略，提供设计意见，以满足定制 IT 和安全的要求 **所提供内容**——网络安全设计开发文件，列举了总体战略和新解决方案规划对安全设计拓扑结构部件和功能进行了定义，包括网络图解和配置样本	**消除网络安全威胁因素** • 确认安全漏洞，根据公司安全策略和业界最佳实践予以调整 • 开发定制网络安全设计，提供多层防御体系以抵御安全威胁 **提高工作效率** • 缩短了新应用和新技术的实施和移植时间 • 避免了设计、实施和部署过程中存在的问题 **降低总拥有成本** • 不必再为支持新的安全需求提供高成本的重新设计 • 为未来的集成和部署初始化作好准备



实施：将安全功能有效地集成入网络基础设施

当您的安全解决方案设计定稿后，思科高级服务专业技术人员将通过实施和部署活动为您的团队提供支持。在规划和设计阶段所提供的健全的安全设计原则和支持，在实施阶段将得以落实，此举将强化您的团队实力，以满足严格的部署日程安排要求，与此同时，最大限度地降低代价高昂的现有网络基础设施中断。

网络安全实施规划审核

如果您正着手规划一项全新安全部署，并希望公司的实施计划获得支持，思科可以帮助您使其进一步开发，在对您的部署项目的目标和范围充分了解之后，思科将就您的计划提供一份报告，对部署、集成和管理安全解决方案所需要的技术流程和资源进行分析。

思科将提示您在实施中可能会遇到的问题，针对软、硬件提供调整建议，以帮助您顺利完成网络阶段化、移植和集成入核心网络基础设施的过程。思科还将为您的测试和安装计划提供支持，并就测试内容、以及如何与专职技术人员合作来验证测试结果而提供建议，从而确保达到接收标准。

表 4 网络安全实施计划审核的特性与优势

功能与措施	优势
功能 • 建立对部署目标、范围和制约因素的理解 • 审核和分析实施计划，包括对解决方案部署、集成和管理的技术和流程的要求 • 审核实施行动计划，包括任务、历史记录、资源和方案 • 分析网络阶段化、测试和安装设计，包括拓扑结构、配置、测试脚本和接收标准 • 软、硬件调整的分析和建议 • 持续分析硬件和配置变化，并通知网络和安全技术人员 **措施** • 举行协作性规划交流，以加强对需求的了解，确认相互依赖关系，确定项目的范围、作用和职责 • 对实施、行动、网络阶段化、测试和安装计划进行研究，并提供建议 • 持续分析网络变化，并通知网络和安全技术人员 **所提供内容**——实施计划评估，为安全解决方案的成功实施与管理提供了建议	**消除网络安全威胁因素** • 为规划最具战略性和有效性的安全解决方案安放和配置提供支持 **提高工作效率** • 强化员工的实力，以满足部署方案的需求 • 最大限度地降低部署过程中现有网络基础设施代价高昂的中断 • 最大限度地降低为支持全新安全解决方案所需付出的代价高昂的网络基础设施重组

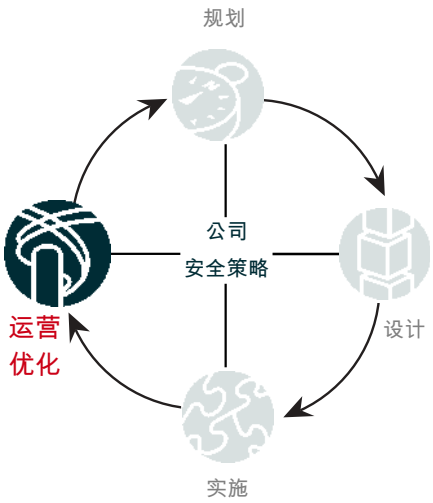
网络安全实施工程

要实现全面的有效性，安全解决方案不仅必须策略性地规划，而且必须周密部署、配置、协调和集成入网络基础设施。思科网络安全高级服务可以帮助公司的技术人员实施全新的安全解决方案（表 5），从而迅速为其环境提供保护，使公司的人力资源得以充分利用。

思科为您实施全新安全解决方案提供了全方位的支持服务。在关键的规划阶段，思科专业技术人员帮助您的公司开发一整套部署战略，包括范围、目标和成功与否的量度，服务内容还包括解决方案部署的详尽计划，如安装、配置、集成和管理。在策略和规划完成后，思科专业技术人员将与您负责实施的员工合作，提供定制安装、配置、测试和协调服务，以确保部署能够顺利地集成入您的生产环境。

表 5 网络安全实施设计的特性与优势

功能与措施	优势
功能 • 研究安全部署项目的目标、范围、要求、资源和限制因素 • 联合开发实施计划，对解决方案部署、集成和管理的技术和流程要求进行详细分析 • 联合开发解决方案测试、安装、配置、集成、管理和维护计划 • 联合开发解决方案部署行动计划，包括任务项目、任务里程和进度表 • 联合开发网络阶段化计划，包括物理和逻辑拓扑结构、配置、测试脚本和接收标准 • 提供解决方案的定制安装、配置、测试、优化和集成服务 • 为与生产网络的集成提供现场支持 • 为员工提供解决方案运营和管理的实际培训 **措施** • 完成项目策划，明确期望、时间表和重要活动，并确定要提供的材料 • 为技术人员执行网络站点调查提供支持 • 在各个现场执行安全解决方案的定制安装、配置、协调和集成 • 为与生产网络的集成提供现场支持 • 与客户技术人员合作，执行实施后认证测试和一日现场支持 **所提供内容**——实施设计报告，对已完成的安装，配置和协调活动进行详细说明，为解决方案的持续运营和管理提供了建议	**消除网络安全威胁因素** • 通过分担部署工作负载，更快速地为公司的商务环境提供保护 **提高工作效率** • 最大限度地降低代价高昂的失误或部署延迟 • 提供高效的解决方案部署，最大限度地利用人力资源 • 从经验丰富的思科安全技术人员处获得必要的实际培训 **降低总拥有成本** • 优化安全解决方案，以进行持续、高效的管理和维护



优化：继续识别和消除风险

在安全解决方案成功部署后，您的网络基础设施将着手为日趋增加的需求作好准备，这是商业动态调整和不断增长的网络需求的必然趋势。随着网络环境的变化，思科将与您合作，共同执行优化审核工作，以帮助确保网络安全基础设施能够继续达到性能目标的要求。

网络安全优化

网络安全优化服务（表6）是在对您的网络和安全基础设施深入了解的基础上建立起来的，而这种了解是通过与您的网络运营技术人员长期合作而获得的，随着网络环境的变化，思科专业技术人员可以利用对趋势和安全突发事件数据的收集与分析，为您的网络提供持续的安全性能评估。

如果您的网络安全偏离了理想状态，思科可以为优化您的安全设计和实施提供调整意见。思科专业技术人员可以对网络安全设备的负载分布和流量处理性能进行评估，提出建议，并提供有关软、硬件的意见，以防止安全违背。如果您准备为网络引入一个全新软件配置，思科专业技术人员可以在部署前，对这些变化的效果进行分析。

思科还提供了网络安全咨询服务，主动向您通知可能会影响您的网络的思科安全专家意见。如果发布安全警报，思科将与您联系，与技术人员合作，来确定对网络的潜在影响，提供网络改进建议，消除安全隐患。

表 6 网络安全优化的特性与优势

功能与措施	优势
功能 • 为包括使用、故障情况、错误阈值和吞吐量在内的网络安全优化定立准则 • 收集和分析可能影响网络安全的趋势和突发事件数据 • 讨论网络安全部件安置和配置，以获得理想的负载分配和流量处理 • 为网络和安全部件的协调提供建议，包括系统优化、过滤、路由重分配、中继和端口配置，以及协议、策略和特性配置 • 监控和审查安全纪录，跟踪系统的使用和值得怀疑的活动 • 提供新软件特性和配置的影响分析 • 提供软硬件建议，优化系统和网络性能 • 确认和分析问题，向技术人员通报网络安全意见 **措施** • 召开规划会议，明确期望、重要活动和要提供的材料 • 为全新软件版本、特性和配置提供持续影响分析 • 提供网络安全问题的持续通报和分析服务 **所提供内容**——实施设计报告，概述网络安全环境的优势与不足，就设计和配置改进提供建议	**消除网络安全威胁因素** • 提出意见，改进网络安全效率，可靠性和性能 • 确保软硬件变化不会影响网络安全 **提高工作效率** • 支持技术人员主动识别和解决潜在的网络安全隐患 • 减少持续通告网络安全漏洞所需占用的时间和资源 **降低总拥有成本** • 优化网络安全基础设施吞吐量和效率

思科在人员、流程、工具和合作伙伴方面的独特优势

思科网络安全高级服务提供了资深专家、深层次的技术知识、专业化的工具和手段，以及业内领先的安全研究试验室，因而可为客户提供高品质的网络安全服务。思科顾问和专业技术人员将与您的团队携手合作，完成对管理不断增长的信息安全隐患发挥关键作用的网络安全解决方案的评估、设计、实施和优化工作，从而将重要企业资产的风险降至最低限度。

如欲了解有关思科高级服务专家如何帮助您消除网络安全威胁因素、提高公司员工工作效率、降低网络总拥有成本的更详尽信息，请与思科销售代表取得联系。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19一21层
邮编：100738
电话：(8610)65267777
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32一33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)87007000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86758000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn

欢迎下载电子文档，http://www.cisco.com/cn/（待定）

2004 年 7 月印刷