思科可管理外部网服务

思科 IT 案例研究/网络/外部网：本案例对思科互联网服务部的可管理外部网服务进行了描述，这是思科 IT 部门为思科内部客户机需要与合作伙伴的外部网连接提供的。思科全球网络是一个领先的企业环境，是世界上最大、最复杂的网络之一。思科客户可以凭借思科 IT 部门在该领域的实际经验，支持类似的企业需求。

“借助获取思科网络资源和流程，一位苏格兰或马来西亚的合作伙伴可以生产出与我们的质量相同的产品，而且生产启动时间也不会延长。这种外部网使我们以低成本生产高质量产品的能力更加突出。”

挑战

思科系统公司®的一个指导方针是关注核心业务以及与合作伙伴的外包合作活动。例如，思科在推出新产品时一开始仅限内部生产，以便研究细节问题，然后，再与负责生产的合作伙伴签约，投入下一步工作。IT 基础设施总经理 Henry White 指出：“合作伙伴提供了世界领先的技术和规模经济，可以确保我们低成本、高利润的优势”。

为了实现日常工作的外包，如生产、工程、财务、技术支持和高级网络服务，思科需要在自身网络和合作伙伴站点间确保安全、价格合理的连接。在推出一款产品前，例如，负责生产的合作伙伴需要接入思科企业资源规划（ERP）系统，以确认设备配置和测试状态，并利用另外一个思科系统打印出厂标签。

思科 IT 互联网服务部（ISG）于 1998 年开始着手开发外部网(Extranet)策略。“我们的任务是提供对内部思科资源的外部网安全接入”，ISG 的 IT 项目经理 Julie Nordquist 说。为解决这个问题，有些公司复制合作伙伴们所需要的全部资源，并将其安装在一个连接到互联网的防火墙之后的安全网络，此处被称为“非军事区”或 DMZ。“由于我们拥有广泛的资源库，创建一个特殊的 DMZ，无论在成本和复杂性方面，都谈不上是一个良好的选择”，她说。相反，思科 IT 部门选择为每位合作伙伴构建了一个独立、安全的可管理网络接入模式来取得所需的共享资源，这些资源受访问控制列表（ACL）保护。

为解决三类连接需求，外部网策略是必不可少的。一类是合作伙伴对思科网络的访问。另一类是思科对这些客户的外部网络的访问，以便进行远程排障和支持。第三类是思科及其合作伙伴间的相互网络访问。

安全和价格合理在设计目标中居重要地位。思科需要保护其资源免遭入侵者和病毒等安全威胁的影响。外部网连接的价格是否合理直接影响到利润，租用专线（通常是帧中继链路）价格之昂贵，在美国本土外更是个致命问题。

解决方案

1999 年，思科在美国部署了第一个外部网连接，用于负责生产的合作伙伴，以及客户网络的远程支持和排障。次年，思科增添了其他类型的外包合作伙伴活动，如工程开发等的外部网连接。2000 年，思科还完成了所有工作区（亚太、美洲、欧洲、中东和非洲）以及位于澳大利亚、印度、中国、日本、荷兰和英国的战略性运作点（POP）的分布式外部骨干网架构的部署工作。在经济发展减缓的 2001 年，思科通过进一步扩展外包活动赢得了效率，这也导致了需要更多的外部网连接。2002 年，思科推出了安全的 VPN 连接，取代租用专线部署，从而大幅度削减了外部网连接成本。

今天，思科外部网为合作伙伴提供了安全、高度可用的思科内部网连接功能，这些公司为思科提供生产、软件开发和呼叫中心功能，以及财务、法律、实施、销售和出版服务。大约有 30%的公司的外部网合作伙伴提供生产服务，并全部集成到了思科供应链应用和流程中。

ISG 的客户端属于思科内部机构，需要外部网接入，以便将合作伙伴和客户连接到思科网络。ISG 将外部网连接作为一项可管理服务而提供，为合作伙伴站点供应和管理思科设备。ISG 向内部客户端机构收取一次性硬件成本，沿用了租用专线连接的线路成本和月度支持的成本。

连接

根据每位客户对可靠性、带宽、支持和成本的具体要求，思科 ISG 部署了三类外部网连接：租用专线、站点间(Site to Site)的 VPN 和基于用户的 VPN。

租用专线

在租用专线连接方面，ISG 提供了配备负载均衡功能的双帧中继租用专线，或一条租用专线作为主链路和基本速率的 ISDN 作为备用，由对性能、可靠性和成本的要求而定。思科 ISG 负责管理该项服务，并为每条外部网链路设定了铂金、金牌和银牌三种不同的服务级别。铂金级服务通常是提供给需要全天服务，或需要提供直接实施或外包“优先级 1”（P1）技术支持等关键或实时功能的合作伙伴。金牌级服务通常是提供给仅在业务时间需要关键支持的合作伙伴，银牌级服务则提供给仅在业务时间需要非关键（尽力而为）支持的合作伙伴。ISG 根据服务级别对思科内部客户端支持成本进行计费。

思科从端到端管理租用专线外部网连接，包括在合作伙伴站点的设备，在思科 POP 部署了一台 Cisco 7206 VXR 路由器，在合作伙伴站点部署 Cisco 3745 多服务接入路由器和 Cisco 3550 交换机。

站点间(Site to Site)VPN

2002 年思科 IT 部门开始在互联网上提供 VPN 连接，以取代租用专线外部网接入。因为这种 VPN 技术削减了月度线路成本，所以显著地降低了外部网连接成本。由于 VPN 已经作为外部网替代选项予以提供，因此，与租用专线相比，VPN 连接的请求比例上升到 5:1。VPN 外部网连接的主要优势是：

- 免除了用于“传统”外部网连接的 WAN 线路成本

- 免除了内部客户机硬件成本，简化了 ISG 库存管理
- 加速了实施
- 方便了短期外部网连接
- 利用基于用户的 VPN 支持从前未配备外部网连接选项的合作伙伴远程工作人员 （见下一部分）

为设置站点间(Site to Site)VPN，思科 ISG 在思科 POP 部署了一台 Cisco 7206 VXR 路由器。在合作伙伴站点，该隧道在思科 ISG 管理的一台 VPN 设备处或合作伙伴管理的一台思科 VPN 路由器处端接。

基于用户的 VPN(Remote Access VPN)

在思科 IT 部门为合作伙伴提供 VPN 外部网选项前，移动的合作伙伴并未真正拥有连接思科内部网资源的能力。现在，当移动用户需要安全接入思科内部网时，思科 ISG 会设置一个基于用户的 VPN。因此，外部网接入是与个人相关、而与站点无关。主办的客户与合作伙伴一道签署一项网络连接协议，另外，用户个人还得签署一项保密协议。在填写具体管理细节后，外部网团队为合作伙伴用户提供验证软件，以便连接到专门供外部网使用的 VPN 集中器。基于用户的 VPN 是一种常用的意外灾害应急措施。例如，如果负责提供技术支持的合作伙伴无法使用普通外部网连接，基于用户的 VPN 则提供了一种接入网络的替代方式，您可以从有效的互联网连接或者完全不同的地点接入网络。目前，美国和亚太地区可以使用基于用户的 VPN。

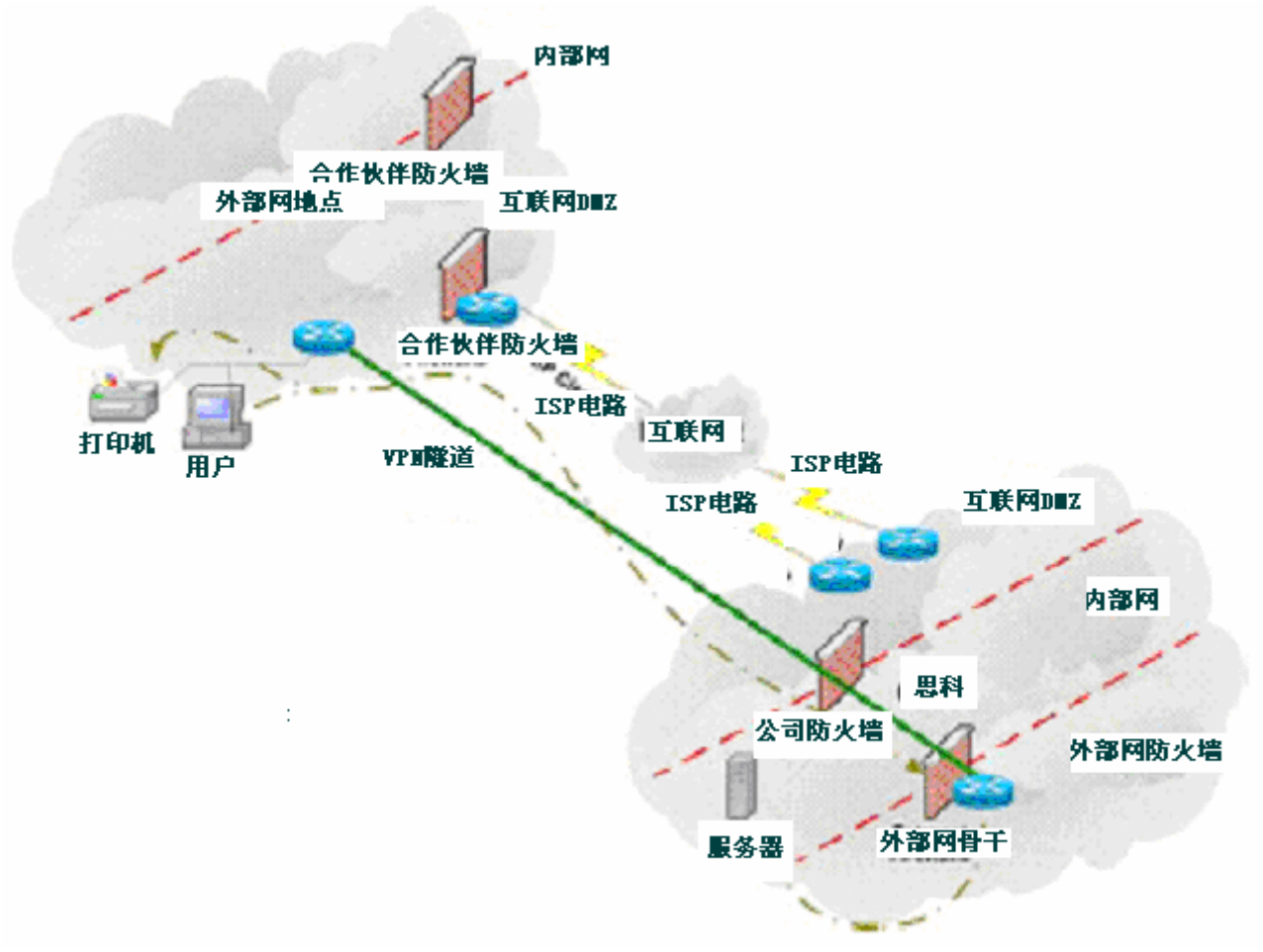
外部网拓扑结构

对于租用专线和基于站点的 VPN 连接，ISG 可以支持远程 LAN 或互联的网络拓扑结构。客户可以根据自己的业务需要进行选择。

远程 LAN 模式

远程 LAN 是位于合作伙伴站点的思科网络的扩展。位于合作伙伴方的可管理思科路由器端接思科的传输连接，并连接到合作伙伴站点的一台或多台可管理交换机（见图 1）。思科内部客户端通常负责提供连接到远程 LAN 的 PC 和打印机。该外部网解决方案是生产、全球定位系统（GPS）和自动监测合作伙伴最通用的手段。“负责生产的合作伙伴通常需要从位于思科站点的服务器打印文件，如果打印机是在他们自己的网络上，而不在思科网络上，就无法完成这一任务”， Nordquist 说。同样，GPS 和自动监测合作伙伴需要在思科远程网络上安装其自己的路由器，以便进行测试。这种远程 LAN 拓扑结构可以隔离思科内部客户机的子网，以使其不会因意外而在生产网络上发送测试数据。

图 1 基于地点的 VPN 外部网的远程 LAN 模式



互联模式

凭借这种互联模式，合作伙伴可以通过与思科 LAN 的互联、连接到自己公司的 LAN 上（见图 2）。位于各方的防火墙负责保护各自公司的资源。合作伙伴可以从其 LAN 上的任意桌面实现连接。与之相比，远程 LAN 模式则仅限于与远程 LAN 连接的物理桌面。一些站点采用了两种拓扑结构。这种灵活性是非常有意义的，例如，如果生产合作伙伴的买方客户可以从自己的桌面访问订购信息，而不必亲自到产品生产区仓库。

图 2 基于地点的 VPN 外部网的互联模式

安全

ISG 与思科信息安全部有着密切的合作关系，以确保外部网连接的安全。“主要问题在于，我们无法控制合作伙伴的周边安全”，公司信息安全经理 Michelle Koblas 说，“如果我们向无足够安全的合作伙伴开放网络，就为进入我们的环境开了一扇后门。”这两个部门合作以消除的潜在风险包括拒绝服务（DoS）攻击、病毒传播、跳转威胁，以及合作伙伴员工断开连接时未能及时通知思科的可能性等。

思科信息安全部就这些问题采取了三项措施：法律手段、接入限制和安全实施。法律手段是指需要外部网合作伙伴签订两项协议。一项是每一个人必须签署的保密协议。另一项是公司范围的网络连接协议，规定了要求合作伙伴公司遵照执行的用户行为和安全策略。

接入限制包括：

- **防火墙准入**——合作伙伴和思科间的思科防火墙在协议的水平上对设备间访问进行了限制。借助路由器中的访问控制列表（ACL），思科在逐个主机和逐项服务的基础上建立了网络间连接。目前，合作伙伴可以对进入网络的流量实施自己的限制。
- **Web 代理**——防火墙使用主机或端口对流量进行了限制：访问一个特定主机的合作伙伴通常可以利用主机上的各项服务，包括 Web、FTP 或 Telnet。思科信息安全部正致力于对 Cisco CSS 11500 系列内容服务交换机的 Web 代理特性的使用进行调查，以便在逐个 URL 的基础上过滤访问。
- **沙箱基础设施**——为防止合作伙伴从一台授权接入的主机“跳转”到另一台未获授权的主机，思科实施了称之为沙箱基础设施的计划，即合作伙伴可以在授权的主机上工作，但该主机不允许向其他主机或网络发送流量。
- **验证和授权**——思科在主机和应用层提供了验证和授权功能。思科信息安全部正在探讨一种方式，即对拥有合作伙伴的授权员工进行定期验证，因此离开该项目的员工不再拥有访问权等等。

总之，凭借入侵检测系统、合作伙伴环境不定期的物理审查，以及周期性 ACL 检查，以确定合作伙伴是否依然需要访问相同主机和服务等的组合，思科完成了外部网安全实施。“我们采用了一种称之为‘深度防御’的模式”，Koblas 说，“换而言之，我们尽可能多地实施安全功能——不仅限于网络级，也包括主机和应用级。”

成效

目前，ISG 支持着全球约 200 个外部网连接，其中大约半数在美国，1/3 用于生产。“1999 年，大约 40%的思科产品是在外部网站点生产的”，White 说，“自从 2000 年，这个部分增长到了 75%。”

思科已从其外部网体验到了可观的业务优势。“通过为合作伙伴提供实时访问数据的能力，外部网改变了我们的业务经营模式”，Nordquist 说，“我们的合作伙伴实时访问订购功能加速了产品推出。”事实上，ISG 最近因其日销售业绩（DSO）创下记录，而受到了思科财务部门的表彰，DSO 是用于度量公司收回款项的速度指标。“我们的外部网为思科赢得了史无前例的业绩——32 DSO 提供了鼎力支持”，White 表示，“我们实现这一财务业绩的能力要归功于世界领先的财务合作伙伴，而外部网正是拥有这些合作伙伴的关键。”

思科外部网还使内部技术支持中心（TAC）员工得以将其专业知识应用到更具挑战性的问题上，而将常规案例交给合作伙伴处理。“80%的 TAC 案例是 Web 生成的”，White 指出，“外部网为我们将这些案例分配给适合处理某类问题的最佳合作伙伴提供了灵活性。”

外部网最大的受益者是思科生产部门。“在接纳一项任务前，思科生产部门会考虑是否合作伙伴能够以更高的效率、更低的成本、更高的质量完成它”，White 说，“如果能的话，我们就会为他们所需的内部资源提供外部网连接。”

下一步

ISG 预计，大量的外部网连接将基于 VPN。为将成本节省进一步扩展至更多的关键合作伙伴活动，如外包 TAC，思科正致力于寻找利用 VPN 技术提供铂金级服务的途径。低成本 VPN 连接，加之以高优先支持，致使合作伙伴的地点变得无关紧要。“凭借获取思科网络资源和流程，一位苏格兰或马来西亚的合作伙伴可以生产出与我们的质量相同的产品，而且生产启动时间也不会延长。这种外部网使我们以低成本生产高质量产品的能力更加突出。”

如需查看思科的各个业务解决方案的更多 IT 案例研究，请访问 Cisco IT@Work 网站：

www.cisco.com/go/ciscoitatwork

注：

本文介绍了思科如何通过部署它自己的产品而获益。本文所介绍的成果和好处可能得益于很多因素；思科并不保证在其他场合下也能取得同样的成果。

思科是以原样提供本文的，不承诺任何明示或者默示的担保，其中包括对适销性或者适用性的担保。有些司法管辖区不允许排除明示或者默示的担保责任。在这种情况下，上述有关排除担保责任的规定可能不适用于您。

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19～21层
邮编：100738
电话：(8610)85155000
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32～33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)85193000
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)86961000
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