

## 终端用户安全指南

# 网络专家多层次的、集成化的网络安全保护

## 目录

互联网是开展业务的理想场所	2
谁是您的网络敌人？	4
您的敌人会做什么？	6
十个简单的安全技巧	9
层次化的安全是有效的安全	10
参考指南	14
速览表	15

## 安全的重要性

互联网是迄今为止全球最大的公共数据网络，它让全世界的个人和企业可以方便地互通信息。它直接影响了地球上几乎每个人的生活——而且它的规模还在日益扩大。

越来越多的通信现在都是通过电子邮件进行。越来越多的移动员工、远程办公人员和分支机构开始利用互联网从远程连接到他们的企业网络——而一些企业的很大一部分收入都来自于通过互联网达成的商业交易。

当然这些都是好消息。但是这个庞大的网络及其相关的技术也给越来越多的安全攻击敞开了大门，而企业必须设法避免受到这种攻击的威胁。

这种攻击的后果是灾难性的——例如可能会丢失非常敏感的信息或者个人数据。对企业或者个人的任何攻击都可能产生非常严重的影响：数据丢失，隐私权受到侵犯，可能还会停机几个小时——甚至几天。即使没有上面所说的那么严重，对网络的攻击也会给企业带来某种原先可以避免的不便。

## 互联网是开展业务的理想场所

尽管安全漏洞会导致风险和成本的提高，但是互联网仍然是最快捷、最方便、最安全的交易场所之一。例如，在某个著名的网站上使用您的信用卡实际上很可能比您在某个餐厅中用它来付款更加安全。但是对安全漏洞的恐惧给很多企业带来了一个严重程度比安全漏洞本身有过之而无不及的问题：对安全性的担忧让很多人不愿意利用互联网进行商业交易。

### 不仅要安全，还要让人感到安全。

为了解决这个问题，企业必须安装和维护安全解决方案，制定安全策略，采取安全措施，这些措施不仅要切实可行——必须要看起来非常有效。企业必须要让他们的客户和潜在客户了解它们在安全方面所做的工作。

随后还需要立法——它越来越成为推动人们对于网络安全的需求的重要因素。各国政府越来越意识到互联网在促进经济增长方面的潜力和犯罪行为对这种增长所能造成的危害。很多国家的政府和国际组织都在制定相关的法律，控制电子数据的传输。与此同时，计算机行业也制定了一系列标准来保护数据和对用户进行身份认证。如果不能严格地遵循这些标准，企业很有可能会受到处罚。

超过 80% 的在线购物者都担心信用卡诈骗问题。
--------------------------

### 您的网络安全面临着哪些威胁？

与其他任何犯罪行为一样，对您的数据的隐私权和完整性的威胁都来自于一小部分人。但是它与其他犯罪的关键区别在于：一个偷车贼一次可能只能盗窃一辆汽车，而一个黑客只需用一台普通的电脑，单身一人就可以导致大范围的——甚至全球范围的——严重破坏。

但是黑客的单枪匹马的形象并不总是十分准确。通常对数据的最严重的威胁都来自于我们认识的人。很多网络安全专家都认为，大部分攻击都是由员工发起的。

无论是由于无意的恶作剧、蓄意攻击还是单纯的失误，经常会有员工设法破坏他们自己的公司的网络，摧毁其中的数据。随着远程办公人员的日益增多，需要保护和监控的网络访问点的个数也会随之不断增加。

了解您的敌人和他们的工作方法一直都非常重要。因此我们将在下一页大致地介绍各种可能会给您的网络带来危险的人员。

## 谁是您的网络敌人？

### 1. 黑客

这个笼统的、含有浪漫意味的词语指得是一些以访问其他人的计算机或者网络为乐的计算机

爱好者。

尽管很多黑客只满足于闯入别人的系统，并留下自己的“脚印”(一些玩笑程序或者信件)，但是有些黑客——被称为“骇客”(cracker)——则怀有很多的恶意。他们会导致整个网络崩溃，窃取或者损坏保密的数据，篡改网页，甚至中断系统的正常工作。

不是所有的黑客都是天才。很多人只需要使用从网上找到的黑客工具，稍微了解一下这些工具的工作方式和作用，就可以发动攻击。

在 2000 年，黑客攻击了 85% 的美国企业和政府机构。

## 2. 没有安全意识的员工

当员工关注于他们各自的工作时，他们可能会忽略标准的网络安全规则。例如，他们可能会选择某个很容易通过简单的常识或者密码破解工具猜测或者破解的密码。

员工还可能会无意地收发和传输病毒。病毒进入系统的最常见途径就是通过受到感染的软件或者从互联网上下载受到感染的文件。

令人惊讶的是，企业还必须注意人为事故的影响。无论员工是计算机新手还是计算机行家，都有可能犯错误，例如错误地安装杀毒软件或者偶然忽略了关于安全威胁的警报。

## 3. 心怀不满的员工

比无心的错误更加让人担心的是某些恼怒的或者意图报复的员工可能对企业造成的损害。恼怒的员工——通常是那些被批评、解雇或者停职的员工——可能会报复性地用病毒感染企业网络，或者有意删除一些重要的文件。

显然这些人非常危险，因为他们通常比较了解企业网络以及其中所含信息的价值，重要信息的位置以及保护这些信息的安全措施。

49% 的公司受到了员工所导致的安全漏洞的影响。

## 4. 喜欢打听消息的员工 (Snoop)

无论员工满意还是不满意，他们中还有些人可能会很好奇，或者喜欢恶作剧。“Snoop”是指那些充当商业间谍的员工；他们会在未经授权的情况下访问机密数据，并将这些信息交给企业的竞争对手。或者他们可能只是很好奇，热衷于访问一些保密的数据，例如财务信息，同事之间发送的浪漫的电子邮件——或者工资的详细信息。

这些行为中有些是无害的。但是另外一些行为，例如事先查看财务、医疗和人力资源数据，则会导致非常严重的后果。它们可能会破坏企业的声誉，提高公司的成本和财务责任。

# 您的敌人会做什么？

## 1. 病毒

病毒是最著名的安全威胁，它是由一些怪癖的程序员编写的计算机程序。它们的独特设计让它们可以在被某个特定事件触发以后自我繁殖并感染计算机软件。

例如，宏病毒可以自动贴附到含有宏指令（可以自动重复执行的命令，例如邮件合并）的文件，并在每次宏指令运行时启动。这些病毒的后果仅仅是让人感到非常厌烦——例如在每次按下某个键时弹出一个好笑的消息。而其他一些病毒则更具有破坏性，可能会导致很多问题——例如降低系统运行速度，或者删除文件。

1999年3月首次在互联网上出现的Melissa病毒位全球的计算机造成了总值八千万美元的损失。

如果从外界引入一个病毒——通过软盘或者某个受到感染的下载文件，该病毒可以感染整个网络。当网络中的某一台计算机感染病毒以后，网络中的其他计算机就非常容易也染上病毒。

## 2. 特洛伊木马程序

特洛伊木马程序，或者简称为特洛伊（trojan），是一些破坏性代码的传输载体。它们表面上看来好像是无害的，但是它们实际上是化装的敌人。它们可能会删除数据，将它们的副本通过电子邮件发送给邮件列表上的其他人，以及去除计算机的保护措施，发动其他攻击。

通过磁盘将特洛伊木马程序复制到系统中，从互联网上下载含有特洛伊木马程序的文件，或者打开电子邮件附件，这些行为都可能感染特洛伊木马。无论是特洛伊木马还是病毒都无法通过电子邮件正文本身传播——只能通过电子邮件的附件。

## 3. 攻击

人们已经发现了各种不同类型的攻击。它们通常可以分为三类：侦察、访问和拒绝服务（DoS）攻击。

- 侦察攻击实际上是一些搜集信息的行为，黑客们需要利用这些信息来攻击网络。像嗅探器和扫描器这样的软件工具可以用图形显示出网络资源的分布状况，发现可能存在的弱点。例如，有一些专门用于破解密码的软件。尽管这些软件的最初目的是合法的，但是在犯罪分子的手中，它们就成了一种非常有效的、危险的武器。
- 访问攻击主要用于发现网络区域中的漏洞——例如身份认证服务和文件传输协议（FTP）功能——以访问电子邮件帐号、数据库和所有保密信息。

西欧的一个喜欢研究在线金融站点的安全性的黑客小组指出：“在当今这个处于金融市场控制之下的世界中，挣钱的最佳途径就是攻击某个企业的形象、声誉和财务信息。”

- DoS 攻击会妨碍用户对整个或者部分网络的访问。它们通常需要发送大量的混乱数据或者无用的数据到某台联网的主机，从而阻止合法的流量通过该主机。破坏性更大的是分布式拒绝服务攻击（DDoS），攻击者将会通过这种攻击威胁多台主机的安全。

#### 4. 破坏性程序（Vandal）

ActiveX 和 Java 应用让 Web 变得更加生动。它们让网站可以利用动画和其他特殊效果来加强吸引力和活动性。但是由于这些应用非常便于下载和运行，所以为破坏行为提供了一种新的载体。破坏性程序是指可以导致不同等级的破坏——从毁坏某个文件到删除计算机系统的大部分内容——的软件应用或者 Java 程序。

拍卖诈骗约占所有在线内容的 43%。
--------------------

#### 5. 数据监听

通过任何一种网络传输的数据都可能会被未经授权的第三方监听。犯罪分子可能会窃听通信内容，甚至更改网络中传输的数据分组。他们可以通过多种方法监听数据、例如，IP 欺骗法可以利用某个接受者的 IP 地址，在数据通信中伪装成一个经过授权的用户。

#### 6. 社交工程

社交工程是指越来越多的利用非技术方式获取保密的网络安全信息的行为。例如，犯罪分子会伪装成一个网络工程师，通过通电话给员工获取密码信息。社交工程的其他例子包括贿赂，或者搜索某个办公室，查找被记录下来的密码。

#### 7. 垃圾邮件（Spam）

垃圾邮件是对各种未经接收方许可就主动发送的电子邮件的统称，其中通常含有广告信息。它一般是无害的，但是非常令人讨厌——而且会占用时间和存储空间。

### 十个简单的安全技巧

1. 鼓励或者要求员工选择比较复杂的密码。
2. 要求员工每 90 天更改一次密码。
3. 确认您的杀毒软件的病毒库是最新的。
4. 向您的员工介绍电子邮件附件的危险性。
5. 实施一个完整的、全面的网络安全解决方案。
6. 定期评估您的安全策略。
7. 在员工离开公司以后，尽快取消他的网络访问权限。
8. 如果您允许员工在家工作，就务必要为远程流量提供一个安全的、集中管理的服务器。
9. 定期升级您的 Web 服务器软件。
10. 不要运行任何不必要的网络服务。

## 更多的层次意味着更加周密的保护

现在我们已经了解到了企业可能面临的威胁和导致这些威胁的人员的情况,因此我们就可以更加方便地制定正确的保护措施和安全策略,从而降低网络出现安全漏洞的可能性。

企业可以从多种技术中进行选择——从杀毒软件包到专用的网络安全硬件,例如防火墙和入侵检测系统。这种多层次的方法有助于在不影响用户快捷地访问网络资源的情况下,保护网络的所有区域。

黑客们在2000年2月对多家著名网站发动了分布式拒绝服务(DDoS)攻击,其中包括Yahoo!, E\*Trade, Amazon.com 和 eBay, 这些攻击导致受到影响的服务器内存溢出,无法响应合法客户的请求。

## 集成化的安全是有效的安全保护措施

### 应用和服务集成



安全连接	周边安全	入侵防范	身份辨识	安全管理
VPN 思科 VPN 集中器 Cisco PIX 防火墙	防火墙 Cisco IOS 防火墙	入侵检测/扫描 Cisco IOS 设备 思科安全扫描工具	身份识别 思科访问控制服务器	策略 Ciscoverks - VPN 管理解决方案 思科安全策略管理器 Web 管理管理器
Cisco IOS VPN	Cisco IOS 防火墙	Cisco IOS IDS		
集成化安全网络基础设施 防火墙 VPN 网络分析 SSL IDS				

思科安全产品系列中的每个产品类别都关系到某个特殊的安全解决方案。

要让一个网络安全解决方案发挥作用,它必须整合不同类型的保护方式,将它们集成到网络的各个部分。安全措施层次越多,在攻击造成损失之前制止攻击的可能性就越大。

在这一节中,我们将集中介绍物理安全的三个最主要的层次:

- 安全连接
- 周边安全

- 入侵防范

## 安全连接

虚拟专用网是公共网络（例如互联网）上的专用连接。它们让用户可以在远离物理网络的地方，以与在企业内部工作时相同的安全等级与企业网络进行通信。如果我们继续用建筑物来比喻网络，那么 VPN 就是一种装甲汽车，它可以沿着公共高速公路将机密信息从外界送到我们所在的建筑物。

所有 VPN 软件和硬件都采用了加密技术，这确保了所传输的消息不会被除了接收者以外的任何人读取。它利用先进的数据算法来“扰乱”消息及其附件。

## 周边安全

如果我们将我们的网络想象成一个建筑物，那么周边安全就像是建筑物周围的围墙和门。

周边安全可以控制用户对于关键性应用、服务和数据的访问，因此只有合法用户和信息可以从一个网络（信任域）进入另一个网络。

## 访问控制

在用户通过密码获得对网络的访问权限之前，网络需要确认他的密码是否有效。访问控制服务器可以检验用户的身份，并根据所存储的用户资料判断用户可以访问哪些区域或者信息。它的作用相当于门口负责检查身份证的警卫。

## 防火墙

防火墙是一种用于限制对网络资源的访问的硬件或者软件解决方案。它就像是一个锁起来的大门——只允许有钥匙（即用户简历和密码）的人进入。

防火墙技术在网络和外部世界之间创建了一个保护层，并可以通过过滤器防止未经授权的或者可能存在危险的信息进入系统。它还可以记录入侵尝试并警告网络管理人员。

## 入侵防范

如果将您的网络想象成一个建筑物，那么入侵防范就相当于监视建筑物周围的围墙的监视摄像机和活动检测器。

一个基于网络的入侵检测系统（IDS）可以提供全天候的网络监控。它可以分析网络中的分组数据流，搜索未经授权的活动——例如黑客攻击——并让用户可以在系统受到影响之前对安全漏洞采取措施。

在检测到未经授权的活动以后，IDS 可以向管理控制台发送含有活动细节的警报，还可以向其他系统发送命令，例如命令路由器切断未经授权的会话。

较低的网络安全水平会给您的企业带来多大的损失？平均每年大约损失两百万美元——这是美国联邦调查局（FBI）最近开展的一项调查得出的结果。

**我们建设了网络。  
我们可以保障网络的安全。**

思科系统公司提供了可以在所有三种安全层次中工作的硬件解决方案。我们的安全模式建立在 SAFE（企业安全架构）文档的基础之上，这些文档是设计和维护安全网络的最佳实践指南。

由于思科开发了互联网所依靠的大部分网络解决方案和产品，因此我们在提供符合当今企业需要的安全解决方案方面拥有独特的优势。

我们在网络领域的专业经验意味着我们可以建设智能化的安全解决方案，它们可以集成到整个公司的网络结构中。

与此同时，我们的安全解决方案的智能足以让我们在网络或者服务受到攻击时主动检测攻击并做出反应。通过在企业网络的架构中采用这种解决方案，企业将可以建立一个智能化的、自保护的网络。

在今天不断变化的市场环境中，网络是企业基础设施中唯一稳定的部分——它会影响到企业的所有系统和服务。今天的客户比以前任何时候都要明确地认识到，网络集成的安全是它们的整个 IT 战略的核心。思科系统公司作为全球最大的网络设备供应商，可以为更多的客户提供比其他任何竞争对手都要多的解决方案。

### 参考指南

● “初学者的网络安全指南”： <a href="http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf">http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf</a>	● 面向安全和 VPN 的 SAFE 蓝图和 Cisco AVVID 虚拟参观： <a href="http://www.cisco.com/go/safepartneretour">www.cisco.com/go/safepartneretour</a>
● 思科 PIX 防火墙： <a href="http://www.cisco.com/go/pix">http://www.cisco.com/go/pix</a>	● SAFE 蓝图网站： <a href="http://www.cisco.com/go/safe">http://www.cisco.com/go/safe</a>
● 公司新闻和信息： <a href="http://www.cisco.com/public/Corp_root.shtml">http://www.cisco.com/public/Corp_root.shtml</a>	● 服务和支持： <a href="http://www.cisco.com/public/Support_root.shtml">http://www.cisco.com/public/Support_root.shtml</a>
● 互联网经济中的教育： <a href="http://www.cisco.com/warp/public/779/edu/">http://www.cisco.com/warp/public/779/edu/</a>	● 服务供应商解决方案： <a href="http://www.cisco.com/warp/public/779/servpro/">http://www.cisco.com/warp/public/779/servpro/</a>
● 政府解决方案： <a href="http://www.cisco.com/warp/public/779/gov/">http://www.cisco.com/warp/public/779/gov/</a>	● 中小型企业解决方案： <a href="http://www.cisco.com/warp/public/779/smbiz/">http://www.cisco.com/warp/public/779/smbiz/</a>
● 入侵检测系统： <a href="http://www.cisco.com/go/ids">http://www.cisco.com/go/ids</a>	● 您的网络的解决方案： <a href="http://www.cisco.com/public/Solutions_root.shtml">http://www.cisco.com/public/Solutions_root.shtml</a>
● “网络安全概述”： <a href="http://www.cisco.com/warp/public/cc/so/neso/sqso/netsp_pl.htm">http://www.cisco.com/warp/public/cc/so/neso/sqso/netsp_pl.htm</a>	● 培训、会议和资源： <a href="http://www.cisco.com/public/Training_root.shtml">http://www.cisco.com/public/Training_root.shtml</a>
● 网络安全网站： <a href="http://www.cisco.com/go/security">www.cisco.com/go/security</a>	● VPN 3000 回收期内的 VPN ROI 计算器： <a href="http://www.cisco.com/go/evpn">http://www.cisco.com/go/evpn</a>

- 产品和技术：[http://www.cisco.com/public/Product\\_root.shtml](http://www.cisco.com/public/Product_root.shtml)

	说明	优势	优点	资源
<p><b>Cisco 3000 VPN 集中器系列 3005 , 3015 , 3030 , 3060 , 3080</b></p>	<p>VPN(虚拟专用网)——通常是一个远程访问系统,可以迅速地取代传统的拨号调制解调器池。利用 VPN,远程用户可以连接到一个互联网服务供应商(ISP)或者一个基于 IP 的专用网络,并在那里通过一个加密隧道,与他们的网络服务器建立一个安全的连接。VPN 还可以用于在 LAN 或者 WAN 中进行安全的通信。</p>	<p>Cisco VPN 3000 集中器系列可以在提高生产率的同时,降低 IT 开支。通过利用共享的服务供应商网络或者互联网,Cisco VPN 3000 集中器无须使用价格昂贵的专线,从而可以大幅度节省开支。与此同时,Cisco VPN 3000 集中器还可以随时随地将移动和远程工作人员安全地连接到他们所需要的工具、人员和信息,从而可以提高生产率。</p> <p>Cisco VPN 3000 集中器系列的三个主要好处:</p> <ul style="list-style-type: none"> <li>● 立即节约开支——由于远程访问 VPN 让用户可以通过本地 ISP 的拨号连接访问网络,而不需要使用价格昂贵的远程连接,所以企业可以立刻节约大量的开支。请利用我们的 VPN 开支节约计算器,计算您所能节约的开支,网址是: <a href="http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/vpn_calc/vpn-start.html">www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/vpn_calc/vpn-start.html</a></li> <li>● 安全的、移动访问——移动工作人员可以利用思科 VPN 客户端和 Certicom Movian VPN 客户端,在家</li> </ul>	<ul style="list-style-type: none"> <li>● 设备外型</li> <li>● 支持硬件客户端</li> <li>● 支持非 Windows 的客户端</li> <li>● 投资保护</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 自动客户端分发</li> <li>● 免费的软件 VPN 客户端</li> <li>● 针对远程访问 VPN 而设计</li> </ul>	<p><a href="http://www.cisco.com/go/evpn">www.cisco.com/go/evpn</a></p>

		<p>或者在外出途中连接到 Cisco VPN 3000 集中器。这些产品让漫游的用户可以通过 PC、手持式个人助理和 CE 设备，安全地访问企业网络。要了解更多关于思科互联网移动办公室解决方案的信息，请访问：<a href="http://www.cisco.com/go/mobileoffice/">www.cisco.com/go/mobileoffice/</a>。</p> <ul style="list-style-type: none"> <li>● 方便的升级——Cisco VPN 3000 集中器是唯一一款用户可以方便地现场升级容量和吞吐量的可扩展平台。</li> </ul>		
<p><b>思科 PIX 防火墙 501 , 506E , 515E , 525 , 535 , Catalyst 6000 防火墙</b></p>	<p>防火墙——一种通过分析进出网络的数据来保护专用网络的方法。防火墙还可以提供网络地址解析功能，从而可以隐藏防火墙内部的计算机的 IP 地址。分组过滤防火墙可以利用基于分组的来源、目的地、端口或者其他基本信息的规则，判断是否允许分组进入网络。</p>	<p>如果您的网络需要连接到互联网，您需要使用一个思科 PIX 防火墙。</p> <p>保障数据和网络资源的安全是电子商务获得成功的关键，而防火墙是一种强制性的网络安全设备。在连接到互联网时，您需要在任何接入互联网的地方安装一个防火墙。思科 PIX 防火墙可以提供无以伦比的安全性、性能、稳定性和方便的安装。</p> <p>思科 PIX 防火墙的三个最主要的好处：</p> <ul style="list-style-type: none"> <li>● 安全性——IX 防火墙是一种针对需求开发的设备，可以提供前所未有的保护等级，它与一种专用的、加固的操作系统紧密集成，这个操作系统中</li> </ul>	<ul style="list-style-type: none"> <li>● 极低的整体运营成本</li> <li>● 防火墙设备外型</li> <li>● 出色的故障恢复性能</li> <li>● 集成的 IDS 特征 ( 50 )</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 管理—特殊设备和整个企业</li> <li>● 最快的防火墙吞吐速度</li> <li>● 免费的 VPN 客户端</li> </ul>	<p><a href="http://www.cisco.com/go/pix">www.cisco.com/go/pix</a></p>

		<p>还集成了状态防火墙和 IP 安全 (IPSec) 虚拟专用网 (VPN) 功能。</p> <ul style="list-style-type: none"> <li>● 性能——PIX 防火墙可以满足大型企业网络和服务供应商的需求。千兆位吞吐量，同时处理 50 万个连接的能力，速度高达 100Mbps 的 IPSec 三重 DES 加密标准 (3DES) 意味着运营级的性能。</li> <li>● 可靠性——通过部署一个冗余的热备用设备，支持高可用性。该设备能够充当一个完全的冗余系统，保持当前的所有会话，从而能够以低廉的价格提供最高的弹性。</li> </ul>		
<p><b>思科安全入侵检测系统</b></p>	<p>入侵检测系统 (IDS) ——一种能够发现、报告可疑的活动，并采取可能的措施，监控某个计算机系统中未经授权的活动的软件，它的作用很像在有人破窗而入时能够鸣叫的家用防盗报警器。IDS 主要分为两类：基于网络和基于主机，它可以监控各个计算机上的日志文件和数据。尽管 IDS 可能会发出很多错误的警报，但是由于防火墙不能阻止所有的入侵者，所以它们正在网络安全中在扮演着越来越重要</p>	<p>不要忘记用入侵检测系统来获得一个更加完整的安全解决方案</p> <p>入侵检测系统 (IDS) 可以监控输入和输出的流量，检测网络攻击并采取相应的措施，因而可以补充设置对网络系统和资产的访问权限的防火墙。层次化安全——包括防火墙和 IDS——是一种健壮的安全。添加入侵检测可以通过创建一个更加全面的安全解决方案，增强您的网络的安全性。</p> <p>入侵检测系统的三个最主要的好处：</p>	<p>思科 NIDS</p> <ul style="list-style-type: none"> <li>● 市场中速度最快的产品</li> <li>● 高度的可靠性</li> <li>● 利用新的 IDM 和 IEV 降低整体运营成本</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 能够采取纠正措施</li> <li>● 可以通过我们新推出的 SILVER 语言进行定制</li> </ul> <p>思科 IDS 主机检测器</p> <ul style="list-style-type: none"> <li>● 基于行为的规则——防范已知的和未知的攻击</li> </ul>	<p><a href="http://www.cisco.com/go/ids">www.cisco.com/go/ids</a></p>

	的角色。	<ul style="list-style-type: none"><li>● 入侵检测可以发现防火墙和虚拟专用网（VPN）没有检测到的攻击。</li><li>● 可以实时监控互联网和外联网连接，保护关键性的资产、系统和资源——相当于现实生活中的监视摄像机。</li><li>● 思科 IDS 可以提供警报，智能化地阻止恶意攻击，甚至动态地重新配置网络，以避免以后再发生类似的攻击。</li></ul>	<ul style="list-style-type: none"><li>● 在主机中建立多个防护层</li><li>● 支持质量</li><li>● 集成到整个安全集成方案中</li><li>● 可扩展性</li></ul>	
--	------	---	--	--

## **北京**

北京市东城区东长安街一号东方广场东一办公楼 19-21 层

邮政编码：100738

电话：(8610) 65267777

传真：(8610) 85181881

## **广州**

广州市天河北路 233 号中信广场 43 楼

邮政编码：510620

电话：(8620) 87007000

传真：(8620) 38770077

## **上海**

上海市淮海中路 222 号力宝广场 32-33 层

邮政编码：200021

电话：(8621) 33104777

传真：(8621) 53966750

## **成都**

成都市顺城大街 308 号冠城广场 23 层

邮政编码：610017

电话：(8628) 86758000

传真：(8628) 65289999