SDN 概述

思科自防御网络(SDN)概述
“有一种网络，它的力量能 —
实现自我保护，更能确保你的业务万无一失
使你的通讯系统融合于一体
更进一步地解放你的生产力
使你轻松获取一切信息
这就是你理想中的网络，现在就是开启它的时候！”

随着公共互联网、电子商务、个人计算机和计算机网络的蓬勃发展，如果不对它们进行妥善的保护，它们将越来越容易受到具有破坏性的攻击的危害。黑客、病毒、不满的员工,甚至人为故障都会给网络带来巨大的威胁。所有计算机用户——从最普通的互联网冲浪者到大型企业——都可能受到网络安全漏洞的影响。但是，通常可以轻松地防范这些安全漏洞。那么怎么防范呢？这本手册将向您讲述最常见的网络安全威胁，以及您和您的企业可以用于防范这些威胁，以及确保您网络中的数据的安全的措施。

互联网无疑已经成为最大的公共数据网络，在全球范围内实现并促进了个人通信和商业通信。互联网和企业网络上传输的数据流量每天都以指数级的速度迅速增长。越来越多的通信都通过电子邮件进行；移动员工、远程办公人员和分支机构都利用互联网来从远程连接他们的企业网络；而在互联网上通过WWW方式完成的商业贸易现在已经成为企业收入的重要组成部分。

尽管互联网已经转变，并大大改进了我们开展业务的方式，但是这个庞大的网络及其相关的技术为不断增长的安全威胁提供了可乘之机，因而企业必须学会保护自己免受这些威胁的危害。尽管人们认为网络攻击者们在入侵存储着敏感性数据（例如个人的医疗或者财务记录）的企业时会比较谨慎，但是对任何对象的攻击所造成的后果包括从轻微的不便直到完全失效——重要数据丢失，隐私被侵犯，网络可能停机几个小时、甚至几天。

如果不考虑这些潜在的安全漏洞所带来的昂贵的风险，互联网可能是最安全的开展业务的手段。但是对于企业来说，对安全问题的恐惧可能会像实际的安全漏洞一样有害。对计算机的恐惧和怀疑仍然存在，相伴而来的是对互联网的不信任。这种不信任可能会限制企业的商业机会，尤其是那些完全基于Web的公司。因此，企业必须制定**安全策略**，采取保护措施，

这些措施不仅要非常有效，而且也要让客户能感觉到它的有效性。企业必须能够以适当的方式向公众说明，他们打算怎样保护他们的客户。 除了保护他们的客户以外，企业必须保护他们的员工和合作伙伴不受安全漏洞的威胁。互联网、内联网、外联网让员工和合作伙伴可以在彼此之间进行迅速的、有效的通信。但是，这种通信和效率必然也会受到网络攻击的影响。对于员工来说，一次攻击可能会导致数小时的停机，而网络必须停止工作，以修复故障或者恢复数据。显然，宝贵的时间和数据的损失可能会大幅度地降低员工的效率和士气。 法律也是推动对于网络安全的需求的另外一股重要力量。政府不仅认识到了互联网的重要性，也认识到，世界的很大一部分经济产值都依赖于互联网。但是他们同时也意识到，敞开世界经济的基础设施可能会导致犯罪分子的恶意使用，从而带来严重的经济损失。各国政府因而制定了相关的法律，以管理庞大的电子信息流量。而且，为了遵守政府所颁行的各项法规，计算机行业也制定了一系列安全标准，以帮助企业确保数据的安全，并证明它的安全性。 没有制定可行的安全策略来保护其数据的企业将无法达到这些标准，并受到相应的惩罚。

"我发现，网络之所以不够安全，通常是由于企业没有制定**安全策略**和利用可以方便地得到的安全工具。企业必须完成**专业的风险评估**，开发**全面的安全计划**和基础设施，这些工作必须得到上层管理人员的公开支持。"
Mark Carter，**COO**，**CoreFacts**，**LLC**，数据恢复和分析公司

所以，制定企业的整体安全策略，是建立“自防御网络”的基础。

随着网络技术不断地发展，网络安全要从以前被动的方式有所转变，在以前，企业不断在已有的计算机网络上不断添加防火墙，网络入侵检测设备，主机防病毒产品，网络身份认证系统，网络管理系统等等，其目的就是要加强网络的安全性，使计算机网络，网络上的通用操作系统，主机应用系统受到不同程度的保护。而今天，思科提出了一个崭新的概念，那就是，安全已经变成了网络的一部分，安全已经和网络密不可分，安全无处不在。而且，今后的计算机网络不但要具有保护网上主机系统，网上终端系统，网上应用系统的能力，关键是要网络本身也具有自我保护能力，自我防御能力，自我愈合能力，一旦受到网络蠕虫，网络病毒的侵扰甚至网络攻击时，能够快速反应，做到网络能够发现攻击，发现病毒，消除蠕虫，做到即保护网络应用的同时，又保护了网络自身，这就是思科所倡导的新一代的“自防御网络”计划 (Self –Defending Network)。

思科自防御网络计划是一种全新的多阶段安全计划，它能够大大提高网络发现、预防和对抗安全威胁的能力。思科自防御网络计划增加了新的系统级威胁防御功能，与通过互联网协议（IP）网络将多种安全服务集成在一起的策略相比，又前进了一步。

以后，该计划还将扩展端点系统和网络安全互操作性，融入动态防感染功能。利用这种新方法，遭受到攻击时，值得信任的端点或其它系统元素可以报告病毒源系统或感染系统的安全问题。思科希望利用这种智能性防止受感染的系统接入网络，从而大大减少病毒、蠕虫和混合病毒的传播。

思科在你身边　　世界由此改变

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一号
东方广场一办公楼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
23层
邮政编码：610017
电话：(8628)86758000
传真：(8628)6528999

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