cisco

Cisco | Networking Academy®
Mind Wide Open™

Course Booklet
思科网络技术学院教程

CCNA 安全

CCNA Security
Version 1.0

[美] 思科网络技术学院 著
北京邮电大学 思科网络技术学

人民邮电出版社
POSTS & TELECOM PRESS

Cisco | Networking Academy®
Mind Wide Open™

Course Booklet
思科网络技术学院教程

CCNA 安全

CCNA Security
Version 1.0

[美] 思科网络技术学院 著
北京邮电大学 思科网络技术

人民邮电出版社
北京

图书在版编目（CIP）数据

思科网络技术学院教程. CCNA安全 / 美国思科网络技术学院著 ; 北京邮电大学译. -- 北京 : 人民邮电出版社, 2011.4
ISBN 978-7-115-24762-9

Ⅰ. ①思… Ⅱ. ①美… ②北… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2011)第002159号

版 权 声 明

思科网络技术学院教程 CCNA 安全

◆ 著　[美] 思科网络技术学院
译　北京邮电大学　思科网络技术学院
责任编辑　李　际

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：19.5
字数：577 千字　2011 年 4 月第 1 版
印数：1－5 000 册　2011 年 4 月河北第 1 次印刷

著作权合同登记号　图字：01-2010-3176 号
ISBN 978-7-115-24762-9

定价：45.00 元

读者服务热线：(010)67132705　印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书所介绍的内容是针对思科网络技术学院最新的认证项目之一——CCNA 安全课程，作为思科网络学院的指定教材，该书面向的读者群需要具备 CCNA 水平的知识。

本书共分 9 章，第 1 章介绍了现代网络安全威胁相关的知识，让大家了解网络安全发展的历史和现状，以及病毒、蠕虫和木马为典型代表的各种攻击的特点和防范。随后的 3 章主要侧重于如何防止外部网络对内部网络的攻击，比如如何加强对路由器的保护、AAA 认证以及防火墙技术和部署。第 5 章介绍了如何对内部网络自身的保护，强调了网络入侵防御系统（IPS）的特点和在思科设备上的实现。第 6 章是针对局域网的安全防护，主要侧重于对于交换网络的安全部署及配置。第 7 章介绍了加密算法，普及了加密技术的基本知识。第 8 章是本书的重要环节，介绍了使用路由器来实现虚拟专用网（VPN）技术，特别是 IPsec 技术的概念和配置。第 9 章综合了前面的内容，介绍了如何设计和部署一个安全网络的全面解决方案，以及如何制定有效的安全策略等。

本书所介绍的内容涵盖了思科国际认证考试——CCNA 安全（IINS 640-553）要求的全部知识，所以，读者也可以把本书作为该认证考试的考试指南。

关于本书

无论是上网还是在实际环境中，本书都是方便阅读、重点突出、便于复习的学习资源。

- 书中文字都从在线教程中提取，使你可以抓住重点。
- 每节的标题可为课堂讨论和考试提供相关在线课程的快速参考。

本书是帮助读者成功完成思科网络学院在线教程的基本的、经济的纸质资料。

致谢

感谢思科网络技术学院的老师参与本书的翻译及校订工作！

北京邮电大学：马刚、王世燕、李涤非、王振华、黄小红
吉林铁道职业技术学院：王爱华
长春大学：邵丹
南京工业大学：韩元

目　录

第 1 章

现代网络安全威胁

本章介绍

网络安全现在已经是计算机网络中一个不可缺少的部分。网络安全包括保证数据安全和消除威胁的协议、技术、设备、工具和技能。网络安全解决方案最早出现于 20 世纪 60 年代，但直到 21 世纪才发展成熟为一套完整的现代网络解决方案。

网络安全的发展动力主要是要领先于怀有不良企图的黑客。正如医生们在治疗已知疾病的同时还要努力预防新的疾病，网络安全工作者在最小化实时攻击造成的影响的同时也要预防攻击。业务的连续性是促进网络安全发展的另一个主要驱动力。

为建立正式社团，网络安全工作者创建了网络安全组织。这些组织设立标准、鼓励协作，并为网络安全人员提供职业发展机会。对于网络安全工作者来说，了解这些组织提供的资源非常重要。

网络安全的复杂性使得要掌握它的全部内容很困难。不同组织创建了多个领域，将网络安全世界划分为多个可管理部分。这样，职业人员就能够在他们的培训、研究和应用中关注于更细分的专业技能领域。

网络安全策略是由公司和政府机构创建，提供给雇员在日常工作中应遵守的框架。管理层的网络安全人员负责创建和维护网络安全策略。所有的网络安全实践都与网络安全策略相关并由网络安全策略提供指导。

就像网络安全由多个网络安全领域组成一样，网络攻击也被分类以便于了解和恰当解决。病毒、蠕虫和特洛伊木马是具体的网络攻击类型。更广义的划分是将网络攻击分为侦查（reconnaissance）、访问（access）或拒绝服务（Denial of Service）攻击。

消除网络攻击是网络安全人员的工作。在本章中，学员将掌握网络安全的基础理论，理解这些基础理论是开始网络安全深入实践所必须的。本章介绍消除网络攻击的方法，这些方法的实现在本课程其余部分介绍。

本章的上机实验“研究网络攻击和安全审计”指导学员对网络攻击和安全审计工具进行研究。实验可以在 cisco.netacad.net 的学院链接（Academy Connection）中的实验手册里找到。

1.1 一个安全网络的基本原则

1.1.1 网络安全的演进

2001 年 7 月，蠕虫“红色代码”攻击了全球的 Web 服务器，感染了超过 35 万台主机。蠕虫不仅使到被感染服务器的访问中断，还影响服务器所在的本地网络，使这些网络速率变得非常慢或不稳定。红色代码蠕虫导致数百万用户遭遇拒绝服务（Denial of Service，DoS）。

如果负责这些被红色代码感染的服务器的网络安全人员制定并实施了安全策略，安全补丁就能够及时得到应用。红色代码蠕虫的影响就能够及早被停止，从而只在网络安全的历史中留下一个脚注。

网络安全与一个组织的业务连续性直接相关。网络安全事故能够影响电子商务，导致业务数据丢失，威胁人们的隐私（以及潜在的法律后果）并危害信息的完整性。这类事故会导致公司资产受损，知识产权失窃，引起诉讼，甚至威胁公共安全。

维护一个安全的网络就确保了网络用户的安全性并保护商业利益。如要保持网络的安全就要求一个组织的网络安全人员保持警惕。安全人员必须时刻了解对网络的新的和正在演进的攻击形式，以及设备和应用程序易遭到攻击的部分。这些信息用于调整、开发和实现消除攻击的技术。然而，网络的安全最终是每个网络使用者的责任。出于这个原因，网络安全人员的工作之一是确保所有用户接受安全意识培训。维护一个安全、受保护的网络为每个人提供了一个更稳定可用的工作环境。

“需要是发明之母。”这句话完全适合于网络安全。在因特网的早期，商业利益是可忽略的。绝大多数用户是研究和开发人员。早期用户很少进行可能伤害其他用户的活动。这时的因特网是一个不需要安全的环境。

在早期，互联网包括通过通信介质连接人和机器。网络人员的工作是将设备连接起来以提高人们交流信息和想法的能力。早期的因特网用户不会花很多时间考虑他们的线上活动是否对网络或对他们自己的数据形成威胁。

当第一批病毒被释放，发生第一次 DoS 攻击时，网络工作者的世界开始发生变化。为了满足用户需求，网络工作者学习保护网络安全的技术。很多网络工作者最初的兴趣来自设计、构建和发展网络来保护已有网络。

今天，因特网与它在 20 世纪 60 年代刚出现时相比已经大为不同。一名网络人员的工作包括确保合适的人员熟练掌握网络安全工具、流程、技能、协议和技术。网络安全工作者保持一种健康的执着态度，以掌握时刻变化着的网络威胁方式非常关键。

随着网络安全成为日常操作不可或缺的一部分，出现了用于特定网络安全功能的设备。

最早的网络安全工具之一是入侵检测系统（Intrusion Detection System，IDS），由斯坦福研究院在 1984 年最先开发。IDS 提供对特定类型攻击发生时的实时探测。该探测允许网络工作者更迅速地消除这些攻击对网络设备和用户造成的负面影响。在 20 世纪 90 年代末期，入侵防御系统（Intrusion Prevention System or Sensor，IPS）开始替代 IDS 解决方案。IPS 设备能够检测到恶意活动并能够自动实时封锁攻击。

除了 IDS 和 IPS 解决方案，防火墙也被开发用来阻止不希望的流量进入网络内的规定区域，从而提供边界安全（perimeter security）。1988 年，数字设备公司（Digital Equipment Corporation，DEC）以报文过滤器的形式创建了第一个网络防火墙。这些早期的防火墙检查报文看它们是否匹配预先设置的规则集，并可以相应地选择转发或丢弃报文。报文过滤防火墙单独检查每个报文，但不检查一个报文是否属于某条现存连接。1989 年，AT&T 贝尔实验室发明了第一个状态防火墙（stateful firewall）。与报文过滤防火墙相同，状态防火墙使用预定义规则来允许或拒绝流量。不同于报文过滤防火墙的是，状态防火墙跟踪已经建立的连接并判断报文是否属于一个已经存在的数据流，从而提供了更高的安全性和更快的处理。

最早的防火墙是向已有网络设备（例如路由器）中添加的软件特性。随着时间的推移，一些公司开发出独立的或专用的防火墙，使路由器和交换机不再进行过滤报文所需的集中占用存储器和处理器的活动。对于不需要使用专用防火墙的组织，可以使用现代路由器，例如 Cisco 集成服务路由器（Integrated Services Router，ISR）作为复杂的状态防火墙。

除了应对来自网络外部的威胁之外，网络人员还必须准备好对付来自网络内部的威胁。内部威胁，不论是有意的还是偶然事故，很可能造成比外部威胁更大的破坏，因为其更了解公司网络和数据，并直接访问公司网络和数据。虽然存在这一事实，在产生消除外部威胁的工具和技术二十多年之后，才

开发出用于对付内部威胁的消除工具和技术。

源自网络内部的威胁的常见场景是一个具备一定技术技能并有破坏意愿的对公司不满的员工。多数来自网络内部的威胁利用了局域网或交换基础设施上使用的协议和技术。这些内部威胁基本上可归入两类：欺骗（spoofing）和 DoS。

欺骗攻击是一台设备通过伪造数据，假装自己是另一台设备的攻击。例如，MAC 地址欺骗的发生就是一台计算机基于另一台计算机的 MAC 地址接收数据报文。欺骗攻击还存在其他一些类型。

DoS 攻击使得网络资源对其预期使用者不可用。攻击者可使用不同方法发起 DoS 攻击。

作为一名网络安全职业人士，理解特别设计用来针对这些威胁类型并确保局域网安全的方法非常重要。

除了预防和拒绝恶意流量之外，网络安全还要求对数据的持续保护。研究和实践如何隐藏信息的密码学被广泛运用于现代网络安全中。现在每一种网络通信都有其相应的协议或技术，被设计用来对预期用户之外的使用者隐藏该通信。

无线数据可以使用不同的密码应用程序加密（隐藏）。两个 IP 电话用户之间的会话可以被加密，计算机上的文件也可以采用加密来隐藏，这只是少数一些例子。密码学几乎可以用在所有存在数据通信的地方。事实上，密码学的发展趋势是所有通信都被加密。

密码学确保了数据的机密性，而机密性是信息安全的 3 个组件之一，另两个组件是完整性和可用性。信息安全关注的是保护信息和信息系统不被未授权访问、使用、泄漏、破坏、修改或毁灭。加密通过隐藏明文数据提供机密性。数据完整性，其含义是数据在任何操作中保持不变，是通过使用散列机制获得。可用性即数据可访问性，由网络硬化机制和备份系统保证。

1.1.2 网络安全的驱动者

“黑客（hacker）”一词有多种含义。对很多人来说，黑客是试图对因特网上的设备进行不经授权的访问的因特网程序员。也指那些运用程序来阻止或减慢大量用户访问网络，或破坏，或擦除服务器数据的个人。但对有些人来说，“黑客”一词也有一种正面的解释，即使用高水平的因特网编程技能确保网络不易遭受攻击的网络专业人士。不论其意义好坏，黑客技术是网络安全的驱动力之一。

从商业角度来看，将恶意黑客的影响减到最小非常重要。当网络很慢或无响应时，商业生产率就会丧失。数据丢失和数据损坏将影响商业利益。

网络安全职业人员的工作是要领先于黑客，要实现领先，他们可以参加培训和专题讨论，参与安全组织，订阅关于威胁的实时反馈以及每天追踪安全网站。网络安全职业人员还必须能够获得先进的安全工具、协议、技能和技术。网络安全职业人员在很多方面应该具备执法者的素质。他们应该时刻保持对恶意活动的警觉，并具有最小化或消除与这些活动相关的威胁的技能和工具。

黑客活动无意中将网络安全职业人员的就业能力和报酬水平提到了很高的位置。然而，与其他技术职业相比，网络安全的学习曲线非常陡峭，并且非常强调致力于持续的职业发展。

黑客行为始于 20 世纪 60 年代，当时的形式是盗用电话线路（phone freaking），或称为飞客（phreaking），指使用多种语音频率操纵电话系统。飞客始于 AT&T 将自动交换技术引入其电话系统之际。AT&T 电话交换机使用不同的音调或音频拨号来指示不同的功能，例如，呼叫结束和拨号呼叫。一些 AT&T 用户意识到通过使用哨音模仿其音调，他们可以利用电话交换机进行免费的长途呼叫。

随着通信系统的演进，黑客技术同样也在发展。20 世纪 80 年代流行起来的战争拨号器（wardialing）使用了计算机调制解调器。战争拨号器程序自动扫描一个本地区域内的电话号码，拨叫每个号码以寻找计算机、电子公告牌系统（bulletin board systems）和传真机。当找到一个电话号码时，将使用密码破解程序来获得访问权。

驾驶攻击（wardriving）开始于20世纪90年代，今天仍然很流行。使用驾驶攻击，用户可通过无线接入点获得对网络的未授权访问。这种攻击使用一辆交通工具和一台无线便携式计算机或PDA。必要时使用密码破解程序进行验证，甚至还有软件用于破解关联到接入点所需的加密方案。

20世纪60年代以来，出现了一批新的威胁，包括Nmap和SATAN这样的网络扫描工具，以及Back Orifice等远程系统管理黑客工具。网络安全职业人员必须熟悉所有这些工具。

因特网上每天有数万亿的美元交易在进行，数百万人的生计依赖于网络商务。基于此原因，制定了刑法来保护个人和企业资产。有大量由于触犯这些法律而使个人不得不面对法律制裁的案例。

第一个电子邮件病毒梅丽莎病毒（Melissa virus）是新泽西州阿伯丁的大卫史密斯完成的。这个病毒导致因特网邮件服务器的内存溢出。大卫史密斯被判在联邦监狱服刑20个月，并被处以5 000美元罚款。

罗伯特莫里斯用99行代码制造了第一个因特网蠕虫。当莫里斯蠕虫（Morris Worm）被发布时，10%的因特网系统停机。罗伯特莫里斯受到指控，被判缓刑3年、400小时公共服务，以及10 000美元罚款。

凯文米特尼克是最有名的因特网黑客之一，由于在20世纪90年代初期非法侵入信用卡账号被监禁4年。

不论是以何种手段进行攻击，例如垃圾邮件、病毒、DoS或强行侵入账号，当黑客把他们的创造性用于恶意目的时，他们的结局往往是被送进监狱，支付大笔罚金，以及不能再访问令他们如鱼得水的网络环境。

这些黑客行为的结果之一是使复杂的黑客工具、政府立法及使网络安全解决方案在20世纪90年代迅速发展了起来。到了20世纪90年代后期，多种复杂的网络安全解决方案被开发出来使各个组织能够在他们的网络内进行战略部署。随着这些解决方案一起出现的还有网络安全领域的新工作机会和增长的报酬。

由于其所需知识的深度和广度，网络安全职业人员的年收入在技术性职业中排名靠前。网络职业人员必须不断更新他们的技能以保持与最新的威胁同步。获取和维持所需知识的挑战经常导致网络安全职业人员的短缺。

网络安全职业人员负责维持一个组织的数据保险（data assurance）以及确保信息的完整性和保密性。一名网络安全职业人员可能需要负责架设防火墙和预防入侵系统，还要确保公司数据加密。实现企业验证方案是另一项重要任务。网络安全工作要求维护网络上可疑活动的详细日志以用于惩戒或起诉违反者。作为一名网络职业人员，熟悉网络安全组织也很重要。这些组织经常发布关于威胁和弱点的最新信息。

1.1.3 网络安全组织

网络安全职业人员必须比其他职业人士更经常地与同行合作。包括参加专题研讨和会议，这类讨论和会议经常与本地、国家或国际技术组织有关，由其赞助或组织。

下面是3个广为接受的网络安全组织：

- 系统管理、审计、网络、安全组织［SysAdmin, Audit, Network, Security (SANS) Institute］；
- 计算机应急反应组（Computer Emergency Response Team，CERT）；
- 国际信息系统安全认证联盟（International Information Systems Security Certification Consortium，(ISC)2读作“I-S-C-squared”）。

其他一些网络安全组织对于网络安全职业人员也很重要。InfoSysSec是一个安全新闻门户网站的网络安全组织，提供与警报、恶意行为及弱点相关的最新重要新闻。Mitre公司维护一个列表，记录著名安全组织使用的常见弱点和暴露的隐患（CVE）。安全组织FIRST将政府、商业组织和教育组织的多

个计算机安全事故响应小组召集到一起，以促进在信息共享、事故预防和迅速反应方面的合作与协调。最后，非营利性组织互联网安全中心（Center for Internet Security，CIS）通过全球在降低商业风险和电子商务中断方面的共识开发安全配置基准。

SANS 是在 1989 年作为合作性的研究和教育组织而建立的。SANS 关注信息安全培训和鉴定。SANS 开发关于信息安全各个方面的研究文档。

从审计员、网络管理员到首席信息安全官，人们分享应对不同挑战的经验教训和解决方案。SANS 的核心是全球从公司到大学各组织的安全从业人员，齐心协力帮助整个信息安全社团。

SANS 资源大部分是可以免费申请到的。包括流行的互联网早期警告系统——互联网风暴中心（Internet Storm Center），每周新闻摘要 NewsBites，每周漏洞摘要@RISK，快速安全报警以及超过 1 200 篇备受赞誉的原创性研究论文。

SANS 开发了安全课程，可用于准备参加审计、管理、运营、法律问题、安全管理及软件安全的全球信息安全认证（Global Information Assurance Certification，GIAC）。GIAC 对安全职业人员的技能进行认证，范围从入门级的信息安全到高级领域，例如审计、入侵检测、事故处理、防火墙和边界保护、数据取证、黑客技能、Windows 和 UNIX 操作系统安全以及安全的软件和应用编码。

CERT 是美国政府资助的，位于卡内基梅隆大学的软件工程学会（Software Engineering Institute，SEI）的组成部分。CERT 与互联网社团一起致力于探测和解决计算机安全事件。莫斯利蠕虫使 CERT 得以在国防部高级研究计划署（Defense Advanced Research Projects Agency，DARPA）的授意下建立。CERT 协调中心（CERT Coordination Center，CERT/CC）关注在安全紧急事件中协调专家之间的交流，以帮助预防未来可能发生的事件。

CERT 对主要安全事件进行响应并分析产品漏洞。CERT 的工作包括管理不断发展的入侵技术和探测攻击，以及如何抓获不断变化难度的攻击者。CERT 开发和推广适用的技术和系统管理实践，来抵挡对联网系统的攻击，限制破坏，并确保服务的连续性。

CERT 专注于 5 个领域：软件保证（software assurance）、安全系统、组织安全、一致反应（coordinated response）、教育和培训。

CERT 传播信息的方式包括发布关于多种安全课题的文章、研究和技术报告、论文。CERT 与新闻媒体一起提高互联网风险意识，并帮助用户了解为保护自己可以采取的步骤。CERT 与其他主要技术组织（例如 FIRST 和 IETF）一起增加对安全性和耐受性的投入。CERT 还向美国政府机构提出建议，包括国家威胁评估中心（National Threat Assessment Center）、国家安全委员会（National Security Council）和国土安全委员会（Homeland Security Council）。

(ISC)2 在超过 135 个国家内提供厂商中立的培训和职业指导服务。它的会员包括全球范围 6 万名经过认证的专业人员。

(ISC)2 的使命是通过将信息安全提升到公共领域，并支持和发展全球范围的信息安全职业人员，使赛博世界成为一个安全的场所。

(ISC)2 开发并维护(ISC)2 公共知识体系（Common Body of Knowledge，CBK）。CBK 定义了全球行业标准，并作为(ISC)2 证书所使用的术语、原理和公共框架。CBK 允许世界范围的职业人士讨论、争辩和解决领域相关的事务。

最值得注意的是，(ISC)2 的 4 项信息安全证书得到普遍认可，包括在网络安全职业界最受欢迎的证书之一——信息系统安全职业人员认证（Certified Information Systems Security Professional，CISSP）。这些证书帮助雇主与经过认证的雇员共同维护信息资产和基础设施的安全。

(ISC)2 通过它的教育和认证，推动了处理安全威胁的专业知识的发展。作为会员，个人可以获得当前的行业信息以及其认证的信息安全职业人员独有的网络机会。

除了各个安全组织的网站之外，对网络安全职业人员最有用的工具之一还包括摘要服务（Really Simple Syndication，RSS）馈送（feed）。

RSS 是一族基于 XML 的格式，用于发布经常更新的数据，例如博客文章、新闻头条、视频和音频。RSS 使用一种标准化的格式。一份 RSS 馈送包括完整或摘要的文本，再加上元数据（例如发布日期和作者身份）。

想要从喜好的网站订阅及时更新馈送或将多个网站的馈送集合到一处的职业人士将受益于 RSS。RSS 馈送可以使用基于 Web 的 RSS 阅读器阅读，RSS 阅读器通常内置于 Web 浏览器。RSS 阅读器软件定期检查用户订阅的馈送是否有更新，并提供接口关注和阅读馈送。通过使用 RSS，一名网络安全职业人员可以每天获得最新信息，还可以随时将实时威胁信息进行聚合以供观察。

例如，US-CERT Current Activity 网页提供定时更新的摘要，记录报告给 US-CERT 的最经常发生的、影响大的安全事件类型。可以使用 http://www.us-cert.gov/current/index.rdf 获得其纯文本格式的 RSS 馈送，该馈送全天随时发送，其信息包括安全公告、电子邮件诈骗、备份漏洞、恶意软件通过社交网站扩散，以及其他潜在威胁。

1.1.4 网络安全领域

对于一名网络安全职业人员而言，理解网络安全的驱动者以及熟悉致力于网络安全的组织是必不可少的。理解网络安全的不同领域也很重要。网络安全领域提供了一个系统的框架，用于促进学习网络安全。

国际标准化组织/国际电子技术委员会［International Organization for Standard ization (ISO)/International Electrotechnical Commission (IEC)］定义了 12 个网络安全领域。根据 ISO/IEC 27002 的描述，这 12 个领域在网络安全的旗帜下，在较高层次上对信息这一广阔范畴进行了组织。这些领域中的一部分明显平行于 CISSP 认证所定义的领域。

这 12 个领域旨在成为开发安全标准和有效管理安全实践的公共基础，并帮助组织间活动建立信任。

网络安全的 12 个领域提供了一种对网络安全要素的便利划分。是否记住这 12 个领域并不重要，重要的是知道它们的存在以及它们是 ISO 正式宣布的。这 12 个领域为网络安全职业人员在工作中提供了有益的参考。

安全策略是其中最重要的领域之一。安全策略是正式声明的规则，被准予访问一个组织的技术和信息资产的人必须遵守这些规则。安全策略的概念、发展和应用在保护组织安全中扮演着非常重要的角色。将安全策略融入一个组织业务运作的各个方面是一名网络安全职业人员的责任。

1.1.5 网络安全策略

网络安全策略是一份全面的端到端文档，能够明确地应用到一个组织的运营中。安全策略被用于辅助网络设计、传递安全原则和促进网络部署。

网络安全策略概述网络访问的规则，确定如何实施策略，并描述组织的网络安全环境基本架构。这种文档通常包含很多页。由于其覆盖的广度和影响，它通常由一个委员会编制。它是一篇复杂的文档，旨在规制诸如数据存取、Web 浏览、密码使用、加密和电子邮件附件等项目。

安全策略应该将恶意用户拒之门外，并能够控制具有潜在风险的用户。当创建了一项安全策略时，必须先理解哪些用户可以使用哪些服务。网络安全策略建立了访问权限的层级，只给雇员以完成其工作所需的最小访问权限。

网络安全策略概述了什么资产需要被保护，并给出了这些资产应该如何被保护的指导。这将被用来确定安全设备、消除策略以及在网络上应该实现的过程。

一个 Cisco 自防御网络（Self-Defending Network，SDN）使用网络来识别、预防和应对威胁。它不同于产品被单独采购而不考虑哪些产品在一起工作会最好的点解决方案策略，基于网络的方法是能

够解决当前挑战并能演进以满足新安全需求的战略性途径。

一个 Cisco SDN 开始于一个强壮、安全、灵活的网络平台，安全解决方案在此平台上建立。一个 Cisco SDN 拓扑包括 Cisco 安全管理器，一个监控、分析和响应系统（Monitoring, Analysis and Response System，MARS），一个或多个 IPS，一台或多台防火墙，几台路由器，以及 VPN 集中器。这其中有的可能是一台 Catalyst 6500 交换机上的刀片或一台集成服务路由器（Integrated Services Router，ISR）中的模块，甚至还可能是安装在服务器上的软件，或者是作为独立的设备存在。

Cisco 集成安全组合（Cisco Integrated Security Portfolio）被设计来满足任何环境、任何网络的需求和形形色色的部署模型。其很多产品可以满足这些要求。

大多数客户不会同时采用 Cisco SDN 的所有组件。由于这个原因，Cisco SDN 提供可以独立部署的产品，并在客户的信心随着每个产品和子系统的应用而建立起来时，提供将这些产品联系起来的解决方案。

Cisco SDN 中的要素可以被集成进网络安全策略中。在创建和修订安全策略时借助 Cisco SDN 方案有助于建立该文档的层级结构。

安全策略在保持其全面性的同时，还应该言简意赅，以便组织中的技术人员能够使用。

创建一项策略的最重要步骤之一是识别关键资产。关键资产可以包括数据库、重要的应用程序、客户和雇员信息、机密商业信息、共享驱动器、邮件服务器和 Web 服务器。

安全策略是公司的一组目标、用户和管理员的行为规则和对系统和管理的要求，所有这些一起确保一个组织中的网络和计算机系统的安全。安全策略是一篇“活的文档”，永远不会结束，并随着技术、业务和雇员的需求变化持续更新。

例如，一个组织的雇员的便携式计算机将遭受不同类型的攻击，如电子邮件病毒，网络安全策略明确定义必须安装病毒软件更新和定义病毒更新的频度。另外，网络安全策略还包括用户可以干什么和不可以干什么的指导。这通常会作为一份正式的可接受的使用策略（Acceptable Use Policy，AUP）在合同中规定。AUP 必须尽可能地明确以避免歧义和误解。例如，一份 AUP 可能会列出被禁止的 Usenet 新闻组。

网络安全策略驱动保护网络资源所需要采取的所有步骤。随着课程的推进，安全策略还会被再次提及，以确保学员理解安全策略在一个管理良好的组织中不可或缺的作用。

1.2 病毒、蠕虫和特洛伊木马

1.2.1 病毒

终端用户计算机最容易遭受的是病毒、蠕虫或特洛伊木马的攻击。

- 病毒是恶意软件，它附着到其他程序，在一台计算机上执行某些的不期望的功能。
- 蠕虫执行恶意代码并将自身的副本安装进被感染计算机的内存，被感染的计算机再次感染其他主机。
- 特洛伊木马是一款经过伪装的应用程序。当一个特洛伊木马被下载并打开时，它从内部攻击终端用户计算机。

传统意义上，病毒一词指的是一种传染性有机体，它需要一个宿主细胞来生长和复制。南加州大学的一名学生 Frederick Cohen 在 1983 年提出了术语“计算机病毒”。计算机病毒（在本课程其余部分称为病毒）是能够复制自身并在用户不察觉的情况下感染计算机的程序。

病毒是一种附着在合法程序或可执行文件上的恶意代码。大多数病毒需要终端用户激活并可以休

眠一段时间，然后在特定的时间或日期发作。简单的病毒可能会把自己安装在一个可执行文件的第一行代码中。当被激活时，病毒可能会检查磁盘并寻找其他可执行文件，这样就可以感染所有它尚未感染的文件。病毒可以无害，例如那些在屏幕上显示一幅图片的病毒；也可以具破坏性，例如那些修改或删除硬盘文件的病毒；病毒还可以被编程具有变异能力以躲避检测。

过去，病毒通常经由软盘和计算机调制解调器传播。现在，多数病毒通过USB存储棒、CD、DVD、网络共享或电子邮件传播。电子邮件病毒是当前最常见的病毒类型。

1.2.2 蠕虫

蠕虫是一种特别危险的恶意代码。它们独立地利用网络中的漏洞复制自身。蠕虫通常会使网络速度下降。

病毒需要有宿主程序才能运行，而蠕虫可以自主运行。它们不需要用户参与，能够以极快的速度传遍网络。

蠕虫导致了因特网上一些最具破坏性的攻击。例如，2003年1月的SQL Slammer蠕虫造成的拒绝服务DoS使全球互联网速度变慢。在它发布的30min内，就有超过25万台主机受到影响。该蠕虫利用了微软SQL服务器的一个缓存溢出漏洞。针对这一漏洞的补丁在2002年中期发布，因此那些被影响的服务器就是没有应用更新补丁的服务器。这个例子很好地说明了，为什么在一个组织的安全策略中需要规定及时对操作系统和应用程序进行更新和打补丁。

尽管这些年出现了一些消除技术，蠕虫仍继续与互联网一起演变并继续对互联网形成威胁。随着时间的推移，蠕虫变得更加复杂，但它们仍倾向于以利用软件应用程序的弱点为基础。大多数蠕虫攻击存在3个主要组成部分。

- **启用漏洞**——蠕虫在易受攻击的系统上利用载体（电子邮件附件、可执行文件、特洛伊木马）安装自身。
- **传播机制**——进入设备后，蠕虫复制自身并定位新目标。
- **有效载荷**——任何能导致某些行为的恶意代码。大多数情况下用于在被感染的主机上创建一个后门。

蠕虫是自包含程序，它攻击一个系统以利用已知的漏洞。一旦利用成功，蠕虫将自身从攻击主机复制到新的被利用系统，开始新的循环。

在对过去20年间的主要蠕虫和病毒攻击的研究中发现，很明显的一点是它们的攻击方法与黑客使用的攻击方法的各个阶段经常很相似。不论是蠕虫还是病毒，都存在5个基本的攻击阶段。

- **探测阶段（Probe phase）**——识别易受攻击的目标，找到可以被破坏的计算机。因特网控制消息协议（Internet Control Message Protocol，ICMP）的ping扫描可以被用来了解网络，然后应用程序扫描和识别操作系统及存在漏洞的软件。黑客可以使用社会工程学、字典攻击、强力攻击或网络嗅探得到密码。
- **穿透阶段（Penetrate phase）**——传送恶意代码到易受攻击的目标，使目标通过一个攻击向量（attack vector）执行恶意代码。攻击向量可以是一个缓冲区溢出、ActiveX或公共网关接口（Common Gateway Interface，CGI）漏洞，或是一个电子邮件病毒。
- **留存阶段（Persist phase）**——当攻击成功地从内存中发起后，代码会尽力留存在目标系统上，以确保即使系统重启，攻击代码仍运行并对攻击者可用。这可以通过修改系统文件、改变注册表或安装新代码来实现。
- **传播阶段（Propagate phase）**——攻击者通过寻找易受攻击的邻近机器试图将攻击延伸到其他目标。传播向量（propagation vector）包括向其他系统发送攻击复制的电子邮件，使用文件共