构建安全与智能的校园网体系

思科校园网络安全解决方案

构筑安全与智能的校园网体系——思科校园网络安全解决方案

随着校园网络规模的不断扩大，网络安全越来越成为园区或校园网络成功运行的关键因素。特别是随着多协议、新业务的发展，网上教学、远程教育、银校一卡通等各种应用使教育网络不再是一个封闭的网络，网络建设中制定网络安全策略，部署相应安全防护方案，保证校园网络的安全顺畅的运行成为迫切需要解决的问题。

本解决方案真对校园网络现阶段所面临的主要安全问题，如：校园网络流量的监控分析，网络攻击的防范，网络病毒的防范，网络流量的控制尤其是严重影响校园网络性能的P2P软件流量的控制提出相应的解决方案，希望能对校园网络安全建设提供建设性的建议和帮助。

校园网络建设现阶段面临的主要问题

随着校园网络规模不断扩大，网络应用不断增加，网络已经成为老师和学生获得信息的主要手段之一，校园网络的规模从以前的几百用户迅速扩充到几千用户甚至几万用户，越来越多的校园网络应用开始部署，网络变得从所未有的重要，一旦网络系统出现问题，5分钟内网络中心的电话就会响个不停，网络的安全和稳定运行给网络中心老师带来很大的压力。通过思科公司对大量校园网络建设案例的跟踪和调查，我们发现现阶段网络建设主要面临以下几方面的问题:

- 网络流量增长得很快，与此同时网络运营商的接入费用不降反升
- 管理人员对校园网的运行情况缺乏基本的分析和管理工具
- 网络安全事件时有发生，重要服务器和核心网络设备被攻击
- 网络病毒泛滥，得不到控制
- 有线用户和无线用户的接入控制，定位缺乏手段

针对这些问题，思科公司建议校园网络建设参考思科自防御网络（Self Defense Network）指导性框架，根据具体情况部署相应解决方案，从而实现校园网络的安全稳定运行。

网络安全与管理的方法

Cisco 自防御网络安全解决方案

思科自我防御网络策略展示了思科安全系统的远景规划。随着面临的攻击的性质不断演化，公司必须采取主动防御措施。过去，来自内部和外部的威胁相对变化较慢，而且比较容易防御。但在现今环境中，互联网蠕虫能在几分钟内迅速散布到全球，安全系统（包括网络本身）必须立即作出反应。

自我防御网络的基础是集成安全——即一个组织的所有方面的本地安全性。在通过分布全球的防御体系来保护网络安全的过程中，每台设备（包括局域网和广域网上的台式机）都在发挥作用。这样的系统有助于确保传输信息的保密性，并能抵御内部和外部攻击；同时还使公司管理员能够控制公司资源的访问。思科实现安全性的方法已经从单点产品演进为集成安全。我们的规划还包括集成其他安全厂商的功能。例如，在思科网络访问控制计划中，思科正在与防病毒厂商携手合作，确保受到病毒感染的设备不能进入网络。在遭到攻击时，这些自我防御网络将能识别各种威胁，并根据其严重级别作出相应反应，隔离遭到病毒感染的服务器和台式机，对网络资源进行重新配置。

思科自我防御网络的远景规划是：将安全连接、威胁防御、信用和身份管理系统集成到单个解决方案中，并提供病毒感染限制、染毒设备隔离功能。

网络安全的关键要素

思科的集成网络安全解决方案包含了有效保护网络安全至关重要的三个要素：攻击防御系统、安全连接系统以及信用和身份管理系统。

攻击防御系统

目前，已知和未知的攻击比过去的攻击破坏性更强，且更为频繁。内部和外部攻击，包括蠕虫、拒绝服务（DoS）、中间人(man-in-the-middle)攻击和特洛伊木马，都能对学校网络造成很大影响。思科威胁防御系统具备强大的防御能力，可以防御已知和未知的攻击。

构筑安全与智能的校园网体系——思科校园网络安全解决方案

要有效地抵御攻击，必须采用相宜的安全技术和先进的网络智能。为了最有效地抵御攻击，这些技术必须在整个网络，而不只是在单点产品或技术中实施，因为攻击可能源于任何一处，并能迅速遍布整个网络资源。思科威胁防御系统提高了现有网络基础设施的安全性，增强了终端（包括服务器和台式机）的全面安全，并将专用的安全技术应用于网络设备和工具中，主动保护业务、应用、用户和网络的安全。威胁防御系统可以防止学校网络运营中断、声誉损失、提高用户满意度。

思科威胁防御系统包括几种关键技术和产品，如防火墙、基于网络的入侵保护传感器、检测仪器、流量隔离技术，能在路由器、交换机和装置中集成安全性。思科安全代理可以提供终端保护。

安全连接系统

网络连接的增加，遭遇攻击的风险也随之增加。随着企业使用互联网来提供企业内联网、外联网和移动办公人员的连接，如“永远在线”的宽带连接，确保这些连接的安全性、数据完整性、保密性就显得极为重要。

局域网连接通常被视为可靠的网络连接，但它现在也需要更高级别的安全性。实际上，内部攻击导致的经济损失比外部攻击高出10倍。保护通过有线或无线局域网传输的数据和应用的机密性和完整性，必须成为企业决策的重要部分。

思科安全连接系统采用加密和鉴权功能，在不受信任的网络上提供安全传输。为保护通过有线和无线介质传输的数据、语音和视频应用，除在思科无线和IP电话解决方案中提供广泛的安全功能外，思科还提供IPSec（IP安全）、SSL（安全套接层）和SSH（安全装置）以及基于MPLS（多协议标记交换）的VPN技术，以确保所有IP通信的保密性。通过集成动态路由、多协议支持和业界最广泛的连接方法，思科解决方案提供了灵活、可靠的连接。

信用和身份管理系统

信用和身份管理系统对电子商务至关重要，它是构建任何安全网络或系统的基础。它负责根据用户的优先权和权利，允许或拒绝对业务应用和网络资源的访问。

思科信用和身份管理系统主要进行基于网络的许可控制。在对用户或设备身份的有效性以及其是否符合公司安全政策等进行验证后，才允许对网络特定资源或特定部分进行访问。网络负责进行身份识别、授权和执行。思科的信用和身份管理解决方案，包括思科交换机和路由器中的思科安全访问控制服务器（ACS）、鉴权协议（如802.1X）和AAA（鉴权、认证和计费）功能，能够灵活地提供高级别访问权限的细节，并能为不符合规定的终端创建隔离区，同时还能拦截所有未授权的访问。

思科公司面向校园园区网络自防御网络蓝图的主要目标是，为用户提供有关设计和实施安全网络的最佳案例信息。自防御网络可作为正考虑其网络安全性要求的网络设计人员的指南。自防御网络在网络安全设计方面采用了深层次自动的防御的方式。这类设计的重点在于所预测出的威胁及自动减轻威胁的方法，而不是单纯地“将防火墙放在这儿，将入侵检测系统放在那儿”等。该策略带来了一种安全分层方式，这样，一个安全系统的故障就不大可能引发对整个网络资源的损坏。自防御网络以思科及其合作伙伴的产品为基础。

自防御网络设计原则与思想

自防御网络基本原则:

- 安全性是过程而不只是简单的产品。
- 网络的所有访问点都是安全性目标。
- 解决安全性与攻击问题的基础应该是综合的安全性策略。
- 成功的安全解决方案要求在整个网络基础设施上采用集成化保护，而不能只考虑某些专用安全性设备。
- 安全解决方案必须能在独立模块中部署，保证提供成本效益、可扩展性和灵活性。

- 通过对服务进行分层安排和提供冗余，自防御网络最大限度减少存在潜在脆弱性的方面。
- 针对关键资源和子网的入侵检测、对关键网络资源的用户和管理员验证与授权。
- 对新兴联网应用的支持。
- 安全性易于管理和报告提供。

网络安全策略

Cisco自防御网络网络安全蓝图将安全架构分解为模块，并为每个模块定义了安全控制。此方式是组织和定义安全要求和推荐解决方案的强大工具。

网络拓扑模块

一般来说，校园园区网将其安全策略和控制分为几类:

- 学校主地点 / 总部核心网络，汇聚网络的安全防护控制。
- 校园网络接入网络模块的安全控制。
- 校园网数据中心，数据中心服务器与互联网间的连接，以及到验证服务器、数据库服务器、应用 / 中间件服务器和内部服务器系统的后端连接，关键服务器的安全防护。
- 互联网模块。到CERNET/其他运营商网络出口的连接，使教职员工能收取电子邮件和上网，安全防护。
- 学校远程接入 / 远程办公者边缘安全性包括但不限于以下模块:
  - 远程接入和虚拟专用网（VPN）模块。提供远程用户对内部网的接入。这些用户一般为员工和内部合同商。
  - 外部网及合作伙伴连接。提供到合作伙伴和供应链厂商的连接。尽管这些连接可能通过电子商务模块提供，外部网模块应有在企业间的第 1 层电路和第 2 层 VPN（如 T1、帧中继等）上保护公司间连接所需的安全拓扑和技术。
  - 其它机构专线接入模块，提供实现其它各办公地点间 WAN 连接所需的安全控制。

Cisco 自防御网络安全架构概述

设计基础

思科安全架构是使网络更安全的建议蓝图。此架构尽可能模拟了当今网络的功能要求。实施决策根据所需网络功能的不同而不同。然而，以下按优先级顺序列出的设计目标对决策制订过程有指导意义。

- 基于策略的安全性攻击缓解
- 整个基础设施（而非仅是专门安全设备上）的安全实施
- 经济有效的部署
- 安全性的管理和报告
- 针对关键网络资源的用户和管理员验证和授权
- 对于关键资源和子网的入侵检测

此架构必须能防止大多数攻击成功影响重要的网络资源。成功突破第一道防线或来自于网络内部的攻击必须被准确发现并得到快速限制，以使其对网络其余部分的影响减至最小。然而，必须在不影响出色网络功能，并提供用户可以依靠的关键服务的情况下提供适当的网络安全性。

在网络设计过程中的许多关键点处，企业必须选择是使用网络设备中的集成功能，还是使用专门的功能设备。集成功能通常较具吸引力，因为它可在现有设备上实施，且这些功能可与设备其余功能互操作以提供性能更出色的解决方案。专门设备通常用于所需功能非常高级或是性能要求使用专门硬件之时。

这些决策应根据专门设备的容量和功能与设备集成优势的比较作出。例如，可能会选择带IOS Firewall的集成化、高容量Cisco IOS®路由器，而非带独立防火墙的较小Cisco IOS路由器。在这个架构中，使用了这两种系统。当设计要求未明确指出特定选择时，设计中就选择集成功能，以便降低解决方案的总成本。

预期的威胁

大多数连至互联网的网络都既有需向外连接的内部用户，也有需接入的外部用户。任何一个方向的连接都可产生入侵者能用于通过第二次尝试而进一步穿越网络的初始突破。大多数攻击来自内部网络。不满的教职员工、学生、竞争对手间谍、好奇访客和粗心的用户都是这类攻击的潜在来源。与互联网相连、可公开接入的主机、也构成了潜在威胁。这些系统常受到应用层易损点攻击和 DoS 攻击。这两种威胁都应在设计安全措施时予以考虑。

模块化方式

尽管大多数网络随机构IT要求的提高而发展，SMB安全架构使用新兴的模块化方式。这种方式有两个主要优点。首先，它使架构在网络的各功能块间建立安全关系，其次，它让设计者可以逐个模块地评估和实施安全性，而不必试图在一个阶段就完成整个架构。每个模块的安全设计独立描述，然后作为整体设计的一部分予以修正。

尽管大多数网络不能简单地划分为明确分开的模块，这种方式为在网络中实施不同安全功能提供了指导。本文不期望网络设计者严格遵照文中的规则，而是建议他们将这些模块的组合集成入已有网络。

网络常规安全性

1、路由器是攻击目标

路由器控制每个网络间的接入。它们连接着可被潜在黑客使用的网络和过滤器。因此，路由器的安全是任何安全部署的关键因素。思科网站上的大量文件提供以下路由器安全方面的具体信息:

- 将 Telnet 接入锁定于一个路由器
- 将 SNMP 接入锁定于一个路由器
- 通过使用 TACACS ＋控制对路由器的接入
- 关闭不需要的服务
- 以适当的级别登录
- 路由更新的验证

2、交换机是攻击目标

像路由器一样，（第 2 层和第 3 层）交换机有自己的安全考虑。尽管没有太多有关交换机中的安全风险以及如何缓解它们的公开信息，但上面描述的大多数安全技术也适用于交换机。此外，以下注意也很重要:

- 无需中继的端口必须将中继设置定为关闭而非自动。这可防止主机成为中继端口而接收所有通常驻留在中继端口上的流量。
- 如果在一个以太网交换机上使用较早的软件版本，那么中继端口应使用交换机中其它端口不使用的虚拟LAN（VLAN）号。这可以防止标有与中继端口相同VLAN 的分组不必通过第 3 层设备就接入另一 VLAN。
- 所有未用的交换机端口都应设置为一个无第 3 层连接的 VLAN。最好将不需要的端口禁用。这可防止黑客插入未用端口并与网络其余部分通信。
- VLAN 不应用作保护两个子网间接入的唯一方式。人员错误的可能，以及VLAN 和 VLAN 标记协议的设计并未考虑安全性的这一事实，使其不适于用于敏感环境。
- 在现有VLAN 中，专用 VLAN 为特定网络应用提供了更高安全性。专用 VLAN 可通过限制 VLAN 中哪些端口能与同一VLAN 中其它端口通信来工作。专用 VLAN 能成为缓解单一受侵害主机的影响的有效方法，但大多数低端以太网交换机还不支持此特性。

3、主机是攻击目标

作为最有可能的攻击目标，主机也提出了某些最为困难的安全挑战。因为主机为其它请求应用服务的主机提供服务，它们在网络中可视性极高。这就是主机最常遭受攻击且在网络入侵尝试中最常被成功侵害的原因之一。

另一主机易损点是其众多硬件平台、操作系统和应用都在不同时期升级和修补。例如，互联网上一个特定Web服务器可能运行来自一个厂商的硬件平台、另一厂商的网卡、来自第三个厂商的操作系统，而web服务器则是开放源或来自其他厂商。此外，这一web服务器可能运行经互联网上免费发布的应用，也可能与另一个同样背景复杂的数据库服务器通信。随着系统复杂度提高，发生故障的可能性也随之提高。

为保护主机，需认真注意系统中的每个元件。使系统与最新补丁、修复等保持同步。特别地，要注意这些补丁是如何影响其它系统元件的运行的。先在测试系统上评估所有更新，再在生产环境中实施它们。如未能这么做，补丁本身就可能导致拒绝服务。典型的应用保护如:

- 服务器主机的基本保护（操作系统未经授权控制、缓存溢出、端口扫描、特洛伊木马等）
- 微软IIS、SQL服务器保护
- DNS、DHCP服务器保护

4、网络是攻击目标

网络攻击属于需处理的最困难攻击之列，因为它们一般以网络运行的方式来利用内在特性。这些攻击包括基于ARP和MAC的第2层攻击、窃听和分布式拒绝服务（DDoS）攻击。部分基于ARP和MAC的第2层攻击可通过交换机和路由器上的最佳实践解决。窃听器在本文末尾有所讨论。DDoS则是一个应受到特殊关注的攻击。

最严重的攻击是无法中止的攻击。DDoS正是如此，DDoS可使数十或数百机器同时向一个IP地址发送大量数据。此攻击的目的一般不是关闭一个特定主机，而是使整个网络无法响应。例如，一个用一条DS1（1.5Mbps）链路连接至互联网、向其网站用户提供电子商务服务的机构，这样的站点对安全性十分注重，有入侵保护、防火墙、记录和有效监控。不幸的是，当黑客启动了一次成功的DDoS攻击时，这些安全设备无一能起到作用。

如果全球100个通过DSL（500Kbps）连接至互联网的设备均得到命令，向远程地址电子商务机构的互联网路由器的串行接口发送信息洪流，即可轻松地用大量数据在DSL上溢流。即使每个主机只能产生100kbps的流量（实验室测试表明一台PC用常用DDoS工具可轻松地生成50Mbps），其总数仍是该电子商务站点可处理的流量的近10倍。因此，合法的web请求被丢弃，站点对大多数用户来说不再运行。本地防火墙丢弃了所有这些大量数据，但那时损害已经造成了。此流量跨越了WAN连接，填满了链路。

只有通过在到校园站点的输出接口上配置限速。限速能在流量超过可用带宽的特定比例时丢弃大多数不需要的流量。关键是正确地将流量标记为不需要。

DDoS攻击的常见形式有ICMP溢流、TCP SYN溢流和UDP溢流。在电子商务环境中，此类流量相当便于分类。只有当在端口80（HTTP）上限制TCP SYN攻击时，管理员才会面临在攻击期间排除合法用户的可能性。即便如此，暂时排除新合法用户、保持路由和管理连接，也要比让路由器过度运行、丢失所有连接好得多。

更多复杂的攻击使用带ACK位集的端口80流量，以便此流量看起来像是合法web流量。管理员不太可能对这样的攻击正确分类，这是因为已认可的TCP通信正是机构允许进入其网络的类型。

限制这类攻击的一个途径就是遵循RFC 1918和RFC 2827中列出的网络过滤准则。RFC 1918定义了预留为专用、永远不应通过公共互联网看到的网络。例如，对于连接至互联网的路由器上的输入流量，可采用RFC 1918和2827过滤来防止未授权流量进入公司网络。当在ISP处实施时，此过滤能防止将这些地址用作源地址的DDoS攻击分组穿越WAN链路，从而在攻击期间节约了带宽。相应地，如果全球的ISP都实施了RFC 2827中的规则，源地址电子欺骗现象就会极大地减少。尽管此战略不直接防止DDoS攻击，但它确实可防止这类攻击对其源地址掩模，这样就较容易跟踪到攻击网络。

5、应用是攻击目标

应用一般由人编码，因此较易出错。这些错误中有的可能危害不大，如导致文件错误打印的错误，但有的也可能是危害极大的恶意错误，如可经由匿名 FTP 获取数据库服务器上的信用卡数据等。恶意错误和其它常见的安全易损点需认真注意。

应注意确保园区网络和公共域应用与最新安全修复同步。公共域应用和定制应用也需要进行代码审查，以保证有缺陷的编程不会带来任何安全风险。这可能包括应用如何调用其它应用或 OS 本身、应用运行的权利级别、应用对周围环境的信任度，以及应用在网上传输数据的方法。入侵检测系统（IDS）可缓解部分针对应用和网络中其它功能的攻击。

入侵检测系统

IDS 起着网络上的报警系统的作用。当 IDS 发现了它认为是攻击的情况时，它或者采取相应行动，或者通知管理系统，向管理员报警以采取行动。

IDS 系统有多种功能来响应和防止攻击。基于主机的入侵检测可通过在单一主机上截获 OS 和应用调用来工作。它也可通过对本地记录文件的事后分析而运作。前一种方式能更好地防止攻击，后一种则是较为被动的攻击响应。

因为职责定义的原因，基于主机的 IDS（HIPS）通常可比网络 IDS（NIDS）系统更好地防止特定攻击，而后者一般只是在发现攻击后发出报警。然而，HIPS 系统也付出了代价：缺乏对整个网络的观察。这种较高的观察角度则是 NIDS 系统的优势。

从理想的角度，思科建议将这两种系统组合——关键主机上安装 HIPS，使用 NIDS 观察整个网络，这样即可获得一个全面的入侵检测系统。不幸的是，IT 预算常常只能允许我们选择其中一种技术。在这种情况下，应对每项技术的总成本、需监控的设备数和需响应攻击的人员认真考虑。

部署 IDS 时，必须调整其实施来提高效率、消除由合法流量或活动引起的“正面误”报警。负面误报警是指 IDS 系统未看到的攻击。调整 IDS 来配置其威胁解决功能。

HIPS 的配置应能在主机级中止大多数验证了的威胁，因为它已做好充分准备来确定某个行动是否确实是威胁。在为 NIDS 选择职责时，第一步是充分调整 NIDS 以确保所有认为的威胁都合法。之后，有两个主要的缓解选项。

第一个选项——如未正确部署则最具破坏力，是通过在路由器上添加接入控制过滤器来“规避”流量。当 NIDS 发现来自特定主机、特定协议上的一个攻击时，它可在预定时间段内阻止此主机进入网络。尽管从表面上看这会对安全管理员有很大帮助，但实际上它需谨慎使用。

规避的主要问题是电子欺骗地址。如果造成攻击的流量被 NIDS 看到，此报警触发了规避，NIDS 将向设备部署接入列表。然而，如果造成报警时攻击使用的是电子欺骗地址，NIDS 现在就锁定拒绝了一个从未发出攻击的地址。如果黑客使用的 IP 地址恰巧是一家大型 ISP 的输出 HTTP 代理服务器的 IP 地址，那么大量用户就无法进入。在一个有创意的黑客手中，这本身就成为很有趣的 DoS 威胁。

为减少规避的风险，它通常应仅用于 TCP 流量，这种流量要比 UDP 难以实现成功的电子欺骗，而且仅用在威胁是真实的且攻击是正面误报警的机率很低的情况下。如果规避时间设置得很短，用户无法进入的时间仅为管理员确定要对此 IP 地址采取什么永久行动（如有）的时间。

在网络内部，存在更多选项。通过有效部署 RFC 2827 过滤，电子欺骗流量应非常有限。此外，因为客户一般不在内部网上，也可以对内部发出的攻击采取限制性更高的态度。而且，内部网络不常有与边缘连接相同水平的状态过滤，所以应在内部环境中更多地依靠 IDS。

NIDS 缓解的第二个选项是使用 TCP 复位。这仅在 TCP 流量上运行，通过向攻击和被攻击主机发送 TCP 复位信息来终止攻击。因为 TCP 流量较难进行电子欺骗，IT 应考虑更多使用 TCP 复位而非规避。TCP 复位在交换环境中的使用要比使用标准集成器时更具挑战性，这是因为在不使用 SPAN 或镜像端口时，所有交换机端口不会看到所有流量。此镜像端口必须支持双向流量并能禁用 SPAN 端口 MAC 学习。

NIDS 观察线上分组。如果分组发送速度快于 NIDS 处理它们的速度，网络性能也不会下降，这是因为 NIDS 不直接位于数据传输过程之中。但是 NIDS 将会失去有效性，分组将被错过，从而导致负面误报警和正面误报警。如想获得 IDS 的全面优势，必须避免此种情况。

像许多状态通晓引擎一样，IDS 在非对称路由环境中不能正确运行。分组从一套路由器和交换机发出，通过另一套路由器和交换机返回，这会导致 IDS 系统只看到流量的一半，导致正面和负面误报警。

安全性的管理和报告

“如果您要记录，就要阅读”，这如此简单，以致于几乎每个熟悉网络安全性的人都至少说过一次。但记录和阅读来自众多设备的信息可能十分具挑战性。

- 哪些记录最重要？
- 我该如何将重要信息与纯粹的通知分开？
- 我应如何确保记录在传输过程中不被干扰？
- 我如何确保当多个设备报告了相同报警时，这些时间标记能相互吻合？
- 如需为犯罪调查提供记录数据，那么到底需要哪些信息？
- 我该如何处理系统在遭受攻击时生成的大量信息？

为有效管理记录文件，所有这些问题都必须得到解答。

从设备管理的角度来看，会提出一系列不同的问题，

- 我如何安全地管理一个设备？
- 我如何向公共服务器推出内容并确保它在传输时不会受干扰？
- 我如何跟踪设备上的改变，在发生攻击或网络故障时纠错？

尽管在其它安全设计指南中描述的“带外”（OOB）管理架构提供了最高级别的安全性，但此处不建议使用，这是因为我们的目标是经济有效地安全性部署。在 OOB 环境中，每个网络设备和主机都有自己的专用管理接口，它们连接至专用管理网络。这降低了在生产网络上传输不安全的管理协议，如 Telnet、TFTP、SNMP 和系统记录的风险（本来很可能被截获或修改）。

在文中介绍的架构上，管理流量在所有情况下都为“带内”传输，并使用隧道协议和不安全管理协议的安全替代品来尽可能实现安全性。例如，在任何可能的情况下，使用 SSH 而非 Telnet。因为管理流量在生产网络中带内传输，严格遵循前面提及的公理是非常重要的。

当需要管理防火墙外的一个设备时，应考虑几个因素。首先，此设备支持哪些管理协议？带 IPSec 的设备应通过简单地创建从管理网络到设备的隧道来管理。这使许多不安全的管理协议可通过单一加密隧道。

当设备上不支持 IPSec 时，必须选择其它不太安全的选项。对于设备的配置，常可用 SSH 或 SSL 来替代 Telnet，以对设备的配置修改进行加密。这些协议有时也可用来取代 TFTP 和 FTP 等不安全协议，为设备推拉数据。然而，思科设备上常需 TFTP 来备份配置或升级软件版本。

这就带来了第二个问题：这一管理通道是否需要一直激活？如并非如此，当执行管理功能时，可在防火墙中放置临时孔洞，再将其移除。但此过程不能扩展至大量设备。

如果此通道需一直激活，那么对SNMP来说，就出现了第三个问题 我是否真正需要此管理工具？SNMP 管理器常用于网络之中，来简化纠错和配置。但对于向两或三个服务器提供第 2 层服务的 DMZ 交换机来说，是否真正需要 SNMP 呢？如答案为否，则可禁用它。

在报告时，大多数网络设备都会发出当对网络问题和安全威胁纠错时非常重要的系统记录数据。此数据应从管理员希望浏览其记录的设备发送至系统记录分析主机。它可实时浏览，或经由按需或事先安排的报告浏览。

根据所涉及的设备，可选择各种记录级别来确保正确数量的数据被发送至记录设备。设备记录数据必须在分析软件中予以标记，以进行具体浏览和报告。例如，在攻击期间，第 2 层交换机提供的记录数据可能不像 IDS 提供的数据那样有吸引力。为确保记录信息同步，主机和网络设备上的时钟必须同步。对于支持它的设备，NTP 保证所有设备都保持准确的时间。处理攻击时，能识别事件发生的顺序是十分重要的。

配置改变管理是与安全管理相关的另一问题。当一个网络处于攻击之下时，重要的是要了解关键网络设备的状态和已知的最后修改发生的时间。变更管理计划应是全面安全策略的一部分，至少变更也应该用设备上的验证系统记录下来，配置应由 FTP 或 TFTP 归档。

安全解决方案架构元件

园区网络安全蓝图中安全解决方案的标准种类如下:

- **身份识别。**身份识别是对网络用户、主机、应用、服务和资源的准确、积极的识别。实现它的标准技术包括验证协议，如 RADIUS 和 TACACS +、Kerberos 和一次性密码工具。数字证书、智能卡和目录服务等新技术正开始在身份识别解决方案中占越来越重要的作用。
- **外围安全 / 接入控制。**它提供了控制到关键网络应用、数据和服务的接入的方法，以便只有合法用户和信息可通过网络。带接入控制列表和/或状态防火墙、以及专用防火墙设施的路由器和交换机提供了这种控制。病毒搜索器和内容过滤器等补充性工具也有助于控制网络外围。
- **数据专用性。**当必须保护信息免遭窃听时，按需提供经验证的保密通信的能力是十分重要的。有时，使用隧道技术，如 GRE 或 L2TP 来进行数据分离，可提供有效的数据私密性。然而，更高私密性要求常需要使用 IPSec 等数字加密技术和协议。在实施 VPN 时，这种添加的保护尤为重要。
- **安全监控。**为确保网络安全，重要的是定期测试和监控安全准备状态。网络易损点搜索器可主动发现弱点领域，IDS 可在发生安全事件时对其监控和响应。利用安全监控解决方案，机构可了解网络数据流和网络的安全状态。
- **策略管理。**随着网络规模和复杂度的增加，对集中策略管理工具的需求也随之提高。带可分析、截获、配置和监控安全策略状态的基于浏览器的用户界面的工具，提高了网络安全解决方案的可用性和有效性。

除安全要求外，网络安全设计还必须具备网络弹性、性能和可扩展性。

参考特性和功能要求

在网络实施过程的很多情况下，需在设备容量和集成功能领域作出选择。集成功能常较具吸引力，因为它可在现有设备上实施，或是因为它可与设备的其余部分互操作，提供功能更出色的解决方案。当需要的功能非常先进和/或性能要求使用专门硬件时，常使用安全设备。选择必须基于安全设备的容量和功能与设备集成优势的比较。此外，管理设备的方式等运行要求可能会影响设备的选择。

参考特性功能要求

职责 / 功能	要求 / 说明
应用服务器	直接或间接为最终用户提供应用服务。服务可包括工作流、日常办公和安全应用。
防火墙	为基于 IP 的协议而维护状态表的状态分组过滤设备。流量仅在符合所定义的接入控制过滤器要求，或属于状态表中已建进程的一部分时能跨越防火墙传输。
主机 IDS	主机入侵检测系统是监控和保护单一主机上行动的软件应用。监控记录可包括修正操作系统和应用呼叫、检查记录文件、文件系统信息和网络连接。
网络 IDS	网络入侵检测系统。此设备一般以无干扰方式运行，可获取 LAN 网段上的流量，并尝试将实时流量与已知攻击特征相匹配。特征包括单一（单分组和方向）特征到需状态表和第 7 层应用跟踪的组合（多分组）特征。
网络分析	可分析、截获、配置和监控安全策略状态的，基于浏览器的用户界面的工具。
Cisco IOS® 路由器	范围广泛的灵活网络设备，为满足所有性能要求提供了许多路由和安全服务。大多数设备是模块化的，且有各种 LAN 和 WAN 物理接口。
第 2 层交换机	在亚太网级为网段提供带宽和 VLAN 服务。一般来说，这些设备提供 10/100Mbps 独立交换端口、千兆位以太网上行链路、VLAN 中继和第 2 层过滤特性。
第 3 层交换机	提供类似于第 2 层交换机的高吞吐率功能，带添加的路由、服务质量和安全特性。模块化交换机常有特殊功能处理器功能。
管理服务器	为网络操作员提供网络管理服务。服务可包括常用配置、网络安全服务监控和安全功能运行。
SMTP 内容过滤服务器	一般运行于外部 SMTP 服务器上的应用，监控出入邮件的内容（包括附件），以便确定该邮件是授权发送、报警发送还是丢弃。
URL 过滤服务器	一般运行于独立服务器上的应用，通过网络设备监控发送给服务器的 URL 请求，并通知网络设备该请求是否应转发到互联网上。这允许 SMB 实施指出哪类互联网站点不能得到授权的安全策略。
工作站或用户终端	直接由最终用户使用的网络设备。这包括 PC、IP 电话、无线设备等。

客户可使用多种产品，其中部分未包括在以下表格中。

Cisco SMB 安全性产品列表

项目 / 产品	职责 / 状态	说明
Catalyst®2950	第 2 层交换机	带安全 LAN 特性的通用交换机
Catalyst®3550	第 3 层交换机	带内部电源和安全 LAN 特性的通用交换机
Catalyst®3750	第 3 堆叠交换机	核心和分布交换机
Catalyst®6509	第 3 层交换机	核心和分布交换机
Cisco 7200 系列	为校园网 Internet 出口提供低速至千兆的安全，稳定的接入	提供从端口从 64k 到 1000 兆。
Cisco 7300	为校园网 Internet 出口提供高速多个千兆的安全，稳定的接入	提供从 100 兆 到 2.5Gbps 的多个端口的连接。
Cisco 7600	为校园网 Internet 出口提供高速多个千兆的安全，稳定的接入	提供从低速 64k 到 2.5Gbps 的高密度、高性能多个端口的连接。
PIX®515/525/535	防火墙及防火墙模块	外围安全性
IDS 4235/4255	网络 IDS 及 IDS 模块	安全监控
Cisco Secure Access Control Server	高性能用户接入控制框架	全面 RADIUS、AAA、TACACS + 和 LDAP 用户验证支持；支持 Cisco 802.1x Catalyst 交换机和无线解决方案
CiscoWorks VPN/Security Management Solution	基于 web 的应用，用于对企业 VPN、防火墙安全性、NIDS 和 HIPS 配置、监控和纠错	配置和监控VPN、PIX防火墙、Cisco IOS路由器和IDS设备；从单一管理控制台监控远程接入VPN，管理PIX防火墙、运行防火墙特性集的Cisco IOS路由器和IDS，而无需丰富的设备或命令行界面（CLI）的知识。

Cisco SMB 安全性产品列表（续）

项目 / 产品	职责 / 状态	说明
WebSense/ SmartFilter	URL 过滤器	过滤输出 URL 请求
内容技术 / NAM	MIME 扫描器，内容分析	过滤进入的电子邮件信息，捕获各项应用数据包
RSA	安全 IDACE	一次性密码服务器
Cisco Security Agent	主机保护 HIPS / HIPS	加载软件CD, 可保护关键服务器免遭已知和未知攻击
用户 PC	Windows/Intel	运行用户应用
服务器	Windows NT/Intel	运行管理和应用
服务器	Solaris	运行管理和应用

自防御网络解决方案设计

我们采用思科的自防御网络解决方案为校园园区网构建网络安全防御体系。

校园网络的流量监控和分析

Internet和大规模部署的校园网络已经为网络管理带来了很多新的挑战。网络出现了很多新的问题，如网络出口拥塞、病毒泛滥和P2P软件滥用网络资源，。作为一位网络专业人士需要监视您校园网络中的关键资源，对性能问题、网络入侵和错误条件进行检测，并能够长期跟踪通信流发展趋势以预测未来的容量需求，需要每天、每周和每月都进行数据的收集。当需要对网络进行扩张或改变时，这些数据的正确格式的报告能够为网络专业人士提供足够的证据，使管理层能够批准项目所需的预算。但是，传统的网络管理工具中还没有一个全面的可对网络的使用情况进行度量的系统。Cisco全面的网络监视工具为网络故障诊断和作出正确决策提供了所必需的性能深入分析，并为未来网络容量的计划提供了基础。

思科公司提供全面的网络监控方案

- 网络第一、二层的流量监控——通过部署 Cisco Works 2000 网管或使用设备内部 Web 管理界面访问设备内置的 RMON 功能实现。
- 网络第三、四层的流量监控——通过部署 Cisco NetFlow 实现详细的流量监控。
- 网络第一至七层的流量监控——通过部署 Cisco Network Analysis Module 实现针对第一至七层内容的监控。

1、交换机，路由器内部的嵌入式 RMON 代理

大多数 Cisco 交换机都装备了嵌入式 mini-RMON 代理，启用这一代理以后，它可以提供基本的网络统计数据，如链路利用率、分组大小分布、冲突、错误分布、以及每一网络端口的广播和组播通信流级别。这些嵌入式 mini-RMON 代理还可以提供利用率的历史视图，并能够通过设置阈值、触发报警和向网络管理基站发送软中断来监视网络中的关键条件。

通过报警和事件群组还可以启用预防性的事先管理功能。现在，网络管理员可以为任何关键统计数据设置阈值，如需要时可以设置每个交换机端口的利用率、组播级别、或故障率阈值。阈值在交换机内取样并进行评估，所以当阈值没有被超过时就不会在网络中产生通信流。当某一阈值被触发时，一个简单网络管理协议（SNMP）软中断将会被发送到网管主机，通知管理员一个重要事件已经发生，而且可能需要采取进一步的措施。

2、Cisco 路由器中的 NetFlow 服务

Cisco IOS 软件交换机制中的 NetFlow 交换功能使 Cisco 路由器 / 交换机能够将高性能的网络层交换与网络服务的应用结合在一起，这些网络服务可以提供安全功能、服务质量（QoS）以及通信流记帐信息。通过 NetFlow 交换功能，可以针对每一个用户和应用提供这些服务。

网络流（NetFlow）的定义是指在给定的源端点和目的地端点之间的IP单播数据报序列。网络流是高度粒度化的；流端点的识别是通过网络三层的IP地址以及网络第四层传输层的应用端口编号。（NetFlow也使用IP协议、服务类型（ToS）和网络接口来识别网络流）。

3、Cisco网络分析模块NAM（Network Analasys Module）
NAM是一个集成的通信流监视解决方案，可以提供全面的RMON I、RMON II、NetFlow和VLAN监视、与协议相关的故障诊断以及趋势分析功能。

交换机中的NAM占用Cisco Catalyst 6500系列交换机的一个插槽。使用流量镜像机制SPAN从Catalyst主干上获得数据来源，收集其它网络设备的Netflow数据，或者从交换引擎中的统计数据中获得数据来源。

路由器中的NAM占用Cisco Catalyst 3800/2800/3700/3600/2600系列路由器的一个插槽。使用流量镜像机制SPAN从路由器主干上获得数据来源，收集其它网络设备的Netflow数据。

NAM的一个关键功能是它能够同时并实时的监控多个交换机端口或VLAN，并能够为每一个数据源提供独立的RMON I/RMON II统计数据。NAM是对交换环境进行监视或故障诊断的理想选择，通过加入象NAM这样的RMON I/RMON II技术，可以使Catalyst 5000系列交换机上的每个以太网、快速以太网和千兆位以太网交换机端口的mini-RMON统计功能得到加强，进而提供全部7个层次的监视功能和强大的钻取故障诊断功能。

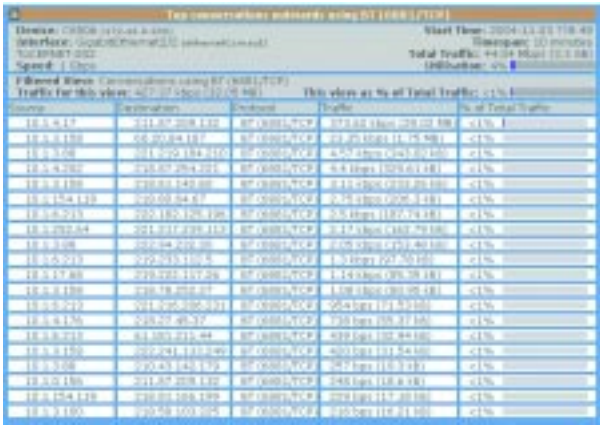
通过部署全面的思科流量分析监控解决方案，校园网管理人员可以轻松的网络监控流量，如:

- 监控网络个端口/VLAN的详细流量分析（利用率、冲突、错误以及分组大小的分布）
- 各种网络应用对网络流量的占用，Top N应用分析
- 分析各个用户对网络的占用，Top N用户分析
- 网络异常流量，如网络病毒的流量分析，定位
- 有多少通信流正在进入我们的Web服务器以及这些通信流从何而来（通信流分析）？
- 网络中什么地方的客户机正在经受因应用服务器导致的延迟?
- 网络中使用P2P软件的用户
- 提供图形化可定制的网络流量报告

思科网络流量监控案例校园网部署实际案例分析

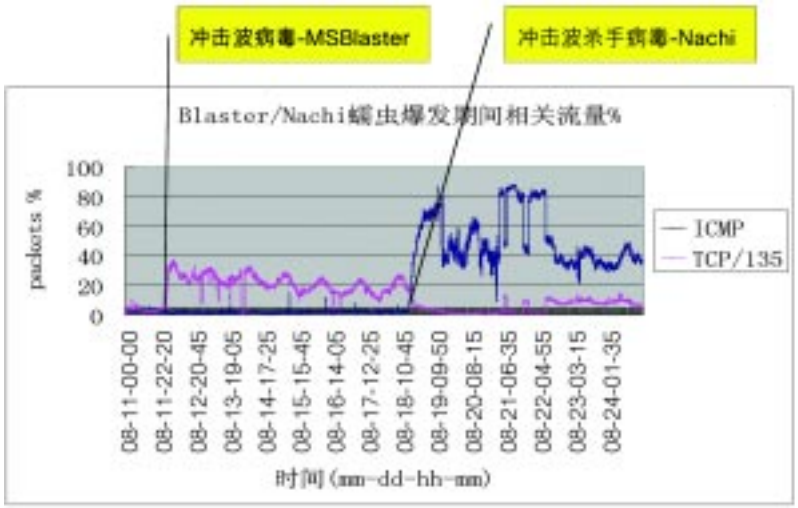
案例一：校园网中使用BT下载软件的用户和流量分析

图1



案例二：网络病毒流量的分析

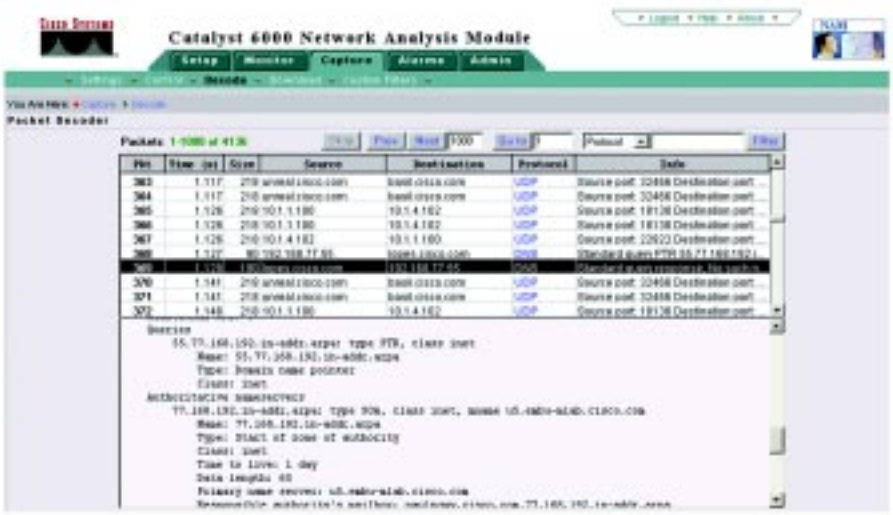
图 2



案例三：故障设备隔离和诊断和保留证据

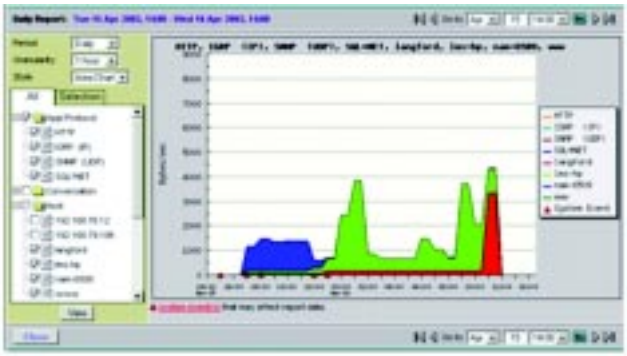
网络管理员可以通过NAM 设定不同网络参数一个域值和意外报警，如过多使用，服务相应延迟，语音质量下降及其他潜在问题。NAM 提供了非常全面的视野对各项应用、客户机、服务器、语音、服务质量等等，同时为迅速隔离网络中故障和不正常工作设备，NAM可以实时捕获并翻译每个数据包。

图 3
实时捕获并解码数据包



案例四：提供灵活的、可客户化的报告功能

图 4



威胁和攻击的防范和缓解

可公开接入的服务器是此模块中最可能遭到攻击之处。以下是可预计的威胁:

- 未经授权接入——通过在 ISP、边缘路由器和公司防火墙的过滤而缓解。
- 应用层攻击——通过主机和网络级的 IDS 缓解。
- 病毒和特洛伊木马攻击——通过电子邮件内容过滤和 HIPS 缓解。
- 密码攻击——限制可强行接入的服务；OS 和 IDS 可发现威胁。
- 拒绝服务——在 ISP 边缘的 CAR 和在防火墙的 TCP 设置控制。
- IP 电子欺骗——ISP 边缘处和中型网络边缘路由器处的 RFC 2827 和 1918 过滤。
- 分组窃听器——交换基础设施和主机 IDS 可限制其爆发。
- 网络探查——IDS 发现探查，过滤协议以限制有效性。
- 信任利用——限制型信任模型和专用 VLAN 可限制基于信任的攻击。
- 端口重定向——限制型过滤和主机 IDS 可限制攻击。

远程接入和站点间 VPN 服务也是此模块中的攻击点。以下是可预计的威胁:

- 网络拓扑发现——入口路由器上的接入控制列表（ACL）可将到 VPN 集中器和防火墙的接入（当用于端接从远程站点发生的 IPSec 隧道）限制为 IKE 和来自互联网的 ESP
- 密码攻击——一次性密码（OTP）可缓解强大密码攻击
- 未授权接入——分组解密后的防火墙服务防止未授权端口上的流量
- 中间人攻击——这些攻击可通过加密远程流量缓减
- 分组窃听器——交换基础设施限制窃听的有效性

以下就几个主要安全防护产品做分别说明。

基于身份认证的网络服务

- 802.1x 思科基于身份的网络服务（Identify Based Network Service）思科基于身份的网络服务IBNS是一种用来增强对基于IEEE802.1X标准构建的企业网络的物理和逻辑访问的安全性的解决方案。Cisco IBNS 是一种基于标准的端口安全性方案，可以由一台 RADIUS 服务器（Cisco Secure ACS）来实现集中化管理。此外，Cisco IBNS 还可以将访问控制和用户安全控制模版数据库相结合，为用户提供更大的灵活性和移动性，确保网络连接、服务和应用的安全性。除了提供动态的基于端口的认证、基于身份来确保安全的网络接入之外，Cisco IBNS 解决方案还能够以用户为单位动态地分配 VLAN 和 ACL。

  在基于 802.1X 的端口安全性之外，思科已经提供并将继续提供一些功能，如端口安全性（Port Security），集成在高端路由器 IOS 中的选择服务网关（SSG）。端口安全特性仍然适用于某些环境中，能够以端口为单位实现网络访问管理，可以在交换机上手工配置。

- PPPoE 虚拟拨号的用户接入方式需要在其用户客户端安装 PPPOE 软件，使用时从客户端（PC 终端）发起 PPP 连接，PPP 连接通过以太网在 PPPoE 终结设备（如路由器）上进行解析后从 PPP 呼叫中提取相应的用户信息（用户名以及密码），将用户信息传递给指定 AAA 服务器上对用户进行认证鉴权，并依据用户情况为用户动态分配合法的 IP 地址，实现 INTERNET 接入。同时 AAA 服务器对用户实施计费，计费可采用时长、流量等多种计费方式，满足不同资费政策的需求。采用 PPPOE 方式解决以太网接入需要安装客户端软件，会造成安装、维护难度增强的问题；同时采用 PPPOE 方式时，由于这是工作在网络第二层的协议，在客户端上 IP 数据会经过 PPPOE、PPP 层协议处理，增加了相应的协议开销，造成有效的通信流量的降低。

- 思科服务选择网关（SSG）让校园网络运营管理者提供可定制的按需服务、知名的 Web 门户（或校园的门户）、基于服务的授权和记帐，以及服务和用户管理。SSG 是 Cisco IOS® 软件的一项功能，可以通过按需提供服务，开辟新的收入渠道。思科 SSG 能为针对不同 IP 目的地的用户交互策略提供 RADIUS 身份认证和记帐功能。这可以为用户带来更高的灵活性和方便性，包括同时登陆多项服务的能力。此外，它还让校园网络运营管理者可以根据用户的连接时间和所使用的服务，向用户收取相应的费用，而不是使用一成不变的价格。有关 SSG 的详细内容介绍参照后文的专门章节。

以上的用户身份认证模式都可以和后台的思科网络注册工具（CNR）配合使用。CNR（Cisco Network Regiterar）是具备丰富功能的 DHCP/DNS 服务器，可以预先设置多种地址分配和解析策略。用户在使用网络资源前，通过各种身份认证方式确认了帐号和密码之后，认证信息被转到 CNR 服务器，该服务器就可根据策略分配合法 IP 地址，如绑定 MAC 地址，基于用户或设备性质分配地址，DHCP 负载均衡和故障恢复等等。

主机保护系统 HIPS

基于主机的入侵检测系统（HIPS）源自于过去人们对于审核日志文件的监控。在传统的系统中，管理员必须在每天结束时查看当天的日志文件，以发现在某个指定的时段内发生的任何恶意行为。这项工作不仅非常繁琐，而且很浪费时间。较新的 HIPS 提供了一个本地代理。它可以执行相同的扫描功能——当某个事件发生时。当该事件被记录到一个日志文件中时，安装在网络资源上的本地软件代理就会检查该事件是否与其攻击数据库中列出的已知特征相匹配。HIPS 还能够监控本地文件的任何变动或者修改。当某个事件符合某个攻击特征时，HIPS 将发送警报并采取措施。

用于服务器和台式机的思科安全代理实现入侵防范的自动防御

思科安全代理可以通过在台式机和服务器上部署有助于防止攻击在网络中蔓延的智能代理，为企业提供强有力的入侵防范能力。与现有的、基于主机的、以攻击为中心（依赖于已知攻击特征的数据库）或以用户为中心（用户访问控制）的安全解决方案不同，思科安全代理是以行为为中心的。通过关注于关键任务型应用的行为，思科安全代理可以防止企业遭受已知的和未知的——后者更加重要——基于主机的安全风险。这可以为用户提供五种重要的优势:

- 台式机和服务器入侵防范——要在安全升级比赛中领先，必要采取预防而非检测。
- 攻击行为的准确预测——如果安全产品无法区分正常行为和恶意行为，它就无法有效地阻止攻击。思科安全代理的自动关联技术及其深层防御方法，使得它几乎不会产生误报。
- 基于行为而非特征——阻止试图采用相同的恶意行为的新型攻击。
- 零升级——思科缺省安全策略可以消除进行繁琐的 HIPS 特征升级的必要性。
- 深层网络安全——将网络上的特征和终端系统上的行为保护结合到一起，层出得保护提供最佳安全性。

思科安全代理可以在攻击生命周期的任何一个阶段防御攻击。通过分析和关联每个阶段的信息，它可以将真正的恶意流量和看上去可疑的（但是合法的）流量区分开。这样做的结果是误报率大幅度下降——通常可以减少 40% 以上。

大部分 HIPS 都会受到误报的困扰。HIPS 供应商可能会建议用户不要让超过 20 到 30 个传感器向同一个管理控制台报告。这不是因为控制台只能处理这么多个传感器，而是因为警报的数量可能会超出操作人员的处理能力。系统真的遭受了这么多的攻击吗？事实并非如此——特征并不完全准确。即使传感器可以通过配置阻塞流量，它也会因为生成过多的误报而无法满足实用需要。

思科安全代理并不依赖于——甚至包含——特征。终端系统安全是由一个管理控制台所定义的策略规则所提供的。这些规则将被分发到位于需要安全的关键服务器和台式机上的智能代理。这些策略规则关注于行为——如攻击生命周期图（图 2）所示，恶意行为的种类相对较少。一个可以防止操作系统被修改的规则将能够阻止很多新的、未知的攻击，因为这些攻击的行为都是修改操作系统。

最后，因为安全保障是基于行为和策略的，因而不需要将任何特征升级分发到代理。这种零升级架构可以在产品的生命周期中大幅度地节约成本。试想一下为了在多个受HIPS保护的关键服务器上升级特征而必须采取的措施——特征必须从供应商处获得。这些特征必须经过实验室测试，以确保它不会影响主机上运行的应用。它必须被部署到服务器上，如果存在某种没有在测试期间发现的、意外的副作用，它就必须被删除。所有这些措施都意味着管理员必须在获取、验证和部署升级特征方面投入大量的时间。升级越多，成本就越高。如果降低升级的频率，成本就会降低，但是主机将会在更长的时间内缺乏保护。

思科安全代理

利用一个像思科安全代理这样的、基于策略的系统，多种终端系统安全问题都会迎刃而解（具体取决于策略的配置方式）。思科安全代理可以解决很多关键的终端系统安全问题:

- 加强服务器和台式机的安全性，包括文件系统和操作系统锁定和完整性保障
- 防止缓冲区溢出和网络攻击
- 保护 Web 服务器
- 台式机分布式防火墙
- 恶意代码箱，可以防止通过Java、JavaScript、ActiveX 或者其他移动代码发动的攻击代理的整合可以为客户带来很高的投资回报。

思科安全代理架构

因为思科安全代理所在的位置很接近内核，因而具有较高的应用可见性。思科安全代理可以利用拦截关联规则引擎（INCORE）技术，拦截系统对于文件、网络和配置资源的所有调用。但是比拦截调用更加重要的是安全代理进行的后续关联操作。这种关联操作和在此基础上的对应用行为的了解将使软件可以真正地阻止新型入侵。

当某个应用需要访问系统资源时，它需要向内核发出一个操作系统调用请求。INCORE 会拦截这些操作系统调用，将其与缓存中存放的一个策略进行比较。这项策略由管理器集中定义（并在代理轮询管理器时下载）。它可以将特定的操作系统调用与应用或者流程的其他行为关联起来，并通过关联这些事件检测恶意行动。如果请求没有违反策略，它将会被发送到内核继续执行。如果请求违反了策略，它将会被阻止（不被发送到内核），而且一个相应的错误消息会被发送回该应用。这时一个警报将会自动生成，并从代理发送到管理器。

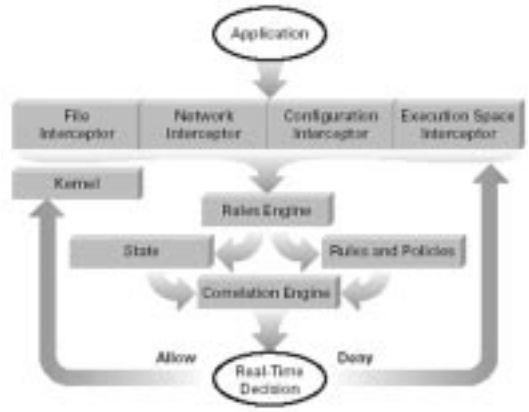
例如，一个 Web 服务器正在提供 HTML 网页服务。在收到来自外部的 Web 请求时，Web 服务器会生成文件系统 I/O 和网络分组 I/O 请求。只要这些请求在策略允许的范围之内（例如 Web 服务器拥有对网页的读取权限），就不会产生任何安全事件。如果某个已知的攻击（例如通过 SSL 加密隐藏的 Unicode 目录穿越攻击）试图以不符合策略的方式使用该应用（例如开启一个命令行解释器程序，如CMD.EXE），该请求将违反策略，并将被阻止。一个错误消息（例如“404:Not Found”）将被生成并发送给远程用户。

假设一个攻击者试图发动一个未知的、以前从未见过的攻击，例如一个缓冲区溢出攻击。这种攻击同样也可以通过 SSL 加密或者逃避技术隐藏起来。执行空间拦截器将会检测到该应用违反了它

自己的或者其他拦截器的执行空间或者文件的规定。在这种情况下，它可以检测到从数据空间执行的代码，并制止这些代码的运行。因为这种行为违反了安全策略，因而无需任何升级就可以制止新的攻击——因而被称为“零升级”。

INCORE（如下图所示）支持四种拦截器:

图 5
思科 INCORE 架构



- 文件系统（所有文件读写请求都被拦截）
- 网络（发生在驱动器[NDIS]或者传输[TDI]级别的分组事件）
- 配置（对于 Windows 中的注册表或者 Unix 中的 rc 文件的读写请求）
- 执行空间

执行空间拦截器并不直接针对某个特定的资源，例如文件或者网络——它的目的是保持每个应用的动态运行环境的完整性。对于不属于发出请求的应用所有的内存的写入请求将被该拦截器发现并制止。一个应用如果试图导入代码（例如导入一个像动态链接库[DLL]这样的共享库）到另外一个流程，也将会被制止。例如，Windows NT 上的 getadmin 漏洞可以利用一种 DLL 导入技术提升用户的权限等级；思科安全代理可以制止这种攻击。最后，这种拦截器可以检测缓冲溢出攻击，防止由此而导致的损失。这样做的结果是，不仅可以保持动态资源（例如文件系统和配置）的完整性，还可以确保高度动态的资源（例如内存和网络 I/O）的完整性。

因为思科安全代理可以拦截文件、网络、配置和运行操作，并将它们与策略相比较，所以它可以跟踪应用的状态。文件、配置和网络操作的组合和队列构成了应用的行为。当一个应用尝试某个操作时，思科安全代理会根据它的策略检查操作，还将把针对该操作的策略与应用的保持关联起来。这使得代理可以根据总体行为实时地做出允许或者拒绝决策，降低因为传统的、无关联的行为制止机制所导致的误报的数量。

思科安全代理策略是IT部门为每个服务器和台式机分配的一组规则。这些以应用为中心的访问控制规则（不是建立在用户或者 ID 的基础上）可以提供对必要资源的安全访问。企业可以方便地部署思科所提供的策略，也可以将其作为专门定制的策略开发的模板。

思科安全代理可以立即为服务器提供重要的入侵防范功能和分布式防火墙功能。这些解决方案非常便于部署，并且可以提供针对多种级别的漏洞的防范和针对常见应用（例如 Microsoft SQL Server、Microsoft Office、即时消息工具和 IIS Web 服务器）的策略。这些策略可以，也应当被立即以最少的配置部署，以保护关键的服务器和台式机。

思科安全代理和多种安全技术

思科安全代理的独特INCORE架构使得它可以充当入侵检测和防范代理，文件完整性监控代理，或者一个应用“沙箱”。拦截器的混合使用（根据管理器上定义的策略）让用户可以创建他们所需要的网络安全应用。根据集中定义的策略规则混用拦截器的能力让思科可以迅速地部署新的终端系统安全功能（如下表所示）。

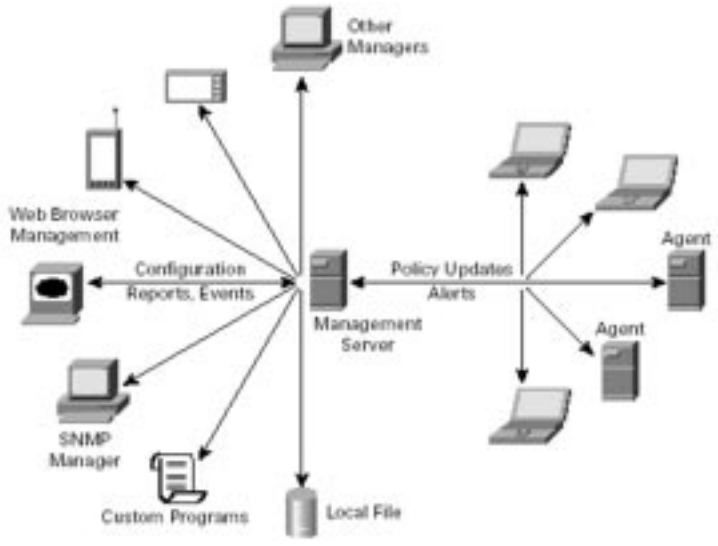
所需要的安全功能	网络拦截器	文件系统拦截器	配置拦截器	执行空间拦截器
分布式防火墙	×			
入侵检测	×	×		×
应用“沙箱”		×	×	×
网络蠕虫防范	×	×		×
系统加固		×	×	

思科安全代理所附带的缺省规则可以部署所有这些网络安全应用（分布式防火墙、IDS、应用“沙箱”等），从而让客户无需自行制定策略。用户可以利用GUI，方便地创建或者更改策略，但是缺省策略可以一次性地提供所有这些保护功能。

因为INCORE提供了几种不同的拦截器，思科安全代理能够提供很多不同的安全功能。通过利用INCORE拦截器的特定组合，用户可以有效地创建传统的安全功能。例如，因为传统的分布式防火墙产品可以阻塞地址和端口，网络拦截器也可以提供这项功能。运营系统加固或者完整性保障关注的是对关键文件或者注册表值的改动，因而这两种阻截器可以提供一种系统加固功能。

思科安全代理管理中心（与VMS 2.2集成）提供了一种代理－管理器（服务器）架构（如下图所示）。其中，策略在管理器上创建和修改，并被自动地分发到所有的代理。管理器使用一个安全的Web界面来管理GUI，从而让用户无需使用不安全的远程访问方式就可以从企业的任何地方进行管理。代理会定期轮询管理器，检查是否存在策略变化或者新软件升级，并实时地向管理器发出警报。代理与管理器之间的所有通信都是安全的，使用了基于标准的协议（安全Web、SSL、基于SSL的HTTP（HTTPS）和TCP端口443）。

图6



后台警报系统非常灵活。代理生成的事件能够通过电子邮件、拨号寻呼机或者简单网络管理协议（SNMP）陷阱发送，并且可以被写入一个本地文件，或者上载到 Cisco VMS SecMon，甚至还可以运行某个设定的程序。很多思科客户都已经成功地将思科安全代理和他们的基于SNMP的网络管理系统（例如Unicenter 和 OpenView）集成到一起，而且思科安全代理管理中心还可以与第三方的管理控制台集成，例如 netForensics。

思科安全代理关联

事件可以在代理上进行本地关联，或者在管理器上进行全局关联。与基于特征的 HIPS 相比，这可以大大提高准确性。

本地管理可以大幅度地减少 HIPS 中普遍存在的误报。通过分析很多不同的行为，可以非常精确地发现恶意行为。一个例子是网络蠕虫的传播。如果蠕虫所执行的每个行为都被独立分析，就会显得一切正常——文件被下载；文件被执行；进程打开 Outlook 地址簿；流程发送电子邮件。其中的每个行为都像是一个每天会出现很多次的、普通的、有效的行为。但是将这些行为串在一起，这些行为就会变得非常危险和具有破坏性。通过关联这些事件，代理能够及时地制止蠕虫的活动，而不会在一天中发出多次警报。不能关联这些事件的 HIPS 则不得不生成诸如“应用 A 开启地址簿”或“A 程序被下载和执行”这样的警报。所有这些事件都必须由管理人员亲自分析，以区分攻击和普通事件。

特洛伊木马的检测是关联功能的另外一个典型例子。跟踪键盘操作或者借助于在线聊天系统（IRC）的通信活动将在一个更加广泛的环境中进行分析，以便在不生成多余误报的情况下检测恶意活动。同样，代理所具有的、根据行为区分应用的能力是一项非常重要的应用控制功能。例如，思科安全代理将把一位类似于一个电子邮件客户端（例如使用对外的邮局协议[POP]、互联网消息访问协议[IMAP]或者简单邮件传输协议[SMTP]）连接的程序视为一个电子邮件客户端。无需将可执行文件的名称（OUTLOOK.EXE）加入一个列表就可以利用各种规则对它们进行控制，例如“电子邮件客户端不能建立对外 HTTP 连接，因为企业政策禁止“Web bug”和“窃听情报”电子邮件进程。”

全局关联功能与之类似，但是它关联的是来自于多个不同的代理的事件。通过分析来自整个企业的事件，可以发现一些有可能被忽视的攻击。这种情况被称为“漏报”。它比误报还要糟糕。向企业中的每台主机发送少量（有时只是一个）分组的攻击者过去可以在不被发现的情况下查明整个网络的结构。利用全局关联功能，这些分布式扫描行为会被代理管理器自动检测出来。如果多个代理检测到同一个程序试图通过电子邮件传播，代理管理器就可以将该程序加入全局隔离列表中。当代理轮询时，它们将会收到经过更新的隔离列表。即使蠕虫还没有对它们发动攻击，蠕虫的可执行文件可能已经被列入这个列表。

网络准入控制

2003 年 10 月，思科与 Network Associates、Symantec 和 Trend Micro 等领先的防病毒软件公司共同制定了网络准入控制计划。这种合作不但能解决当今企业客户面临的各种安全问题，还能降低蠕虫和病毒发作后的修复成本。

最近，随着蠕虫和病毒感染的增加，用户提出了怎样防止不安全节点访问受感染网络的问题，对当今的所有大企业来讲，这都是个大问题。目前，许多机构都能够成功地在自己的互联网范围内对付蠕虫攻击，但是，当移动用户或客户直接将其受感染PC与内部局域网连接时，仍有可能遭到病毒攻击。要消除这种威胁，不但要加强安全策略的实施，还应该采用思科正在提供的网络准入控制技术。

借助 NAC，客户可以只允许值得信任的兼容终端设备（例如 PC、服务器和 PDA）接入网络，同时限制不兼容设备的接入范围。在第一阶段，当端点设备试图与网络连接时，路由器将能够通过NAC限制接入权限。决策的依据是终端设备的信息，例如当前防病毒状态以及操作系统补丁水平。NAC 可以禁止不兼容设备接入，将其放置在隔离区，或者只允许它有限访问计算资源。一开始，NAC 将支持运行 Microsoft®Windows NT、XP 和 2000 操作系统的 PC 终端。

以远程用户和移动用户形式出现的未知计算的增加给战略性信息资产带来了很大的安全威胁。借助思科与防病毒软件公司的合作，将能够对接入网络的计算机实行统一的安全策略。网络准入控制将能够充分利用我们在安全软件和网络基础设施上的现有投资，保证接入网络的计算机符合共同的安全策略。

NAC 的关键组件是思科开发的称为 Cisco® Trust Agent 的软件，它驻留在终端系统上，与思科网络通信。Cisco Trust Agent 的作用是从多个安全软件客户端收集安全状态信息，例如防病毒客户端，然后将这些信息传送到思科网络，在那里制定和实施准入控制决策。思科已经向 Network Associates、Symantec 和 Trend Micro 授予了 Cisco Trust Agent 技术的使用许可证，以便这些厂商能够将 Cisco Trust Agent 与其安全软件客户端产品集成在一起。思科及其 NAC 合作公司计划免费向客户提供 Cisco Trust Agent。另外，Cisco Trust Agent 还将与 Cisco Security Agent 集成在一起，以便按照终端设备的操作系统补丁水平实施接入权限。Cisco Security Agent 是思科笔记本/台式机和服务器的主机入侵防护和分布式防火墙软件，用于及时发现和预防恶意行为。

防火墙

防火墙的传统角色已经发生了变化。今天的防火墙不仅可以保护企业网络免受未经授权的外部接入的攻击，还可以防止未经授权的用户接入企业网络的子网、工作组和 LAN。FBI 的统计数据显示，70% 的安全问题都来自于企业内部。在 FBI 开展的调查中，五分之一的受访者表示，在过去 12 个月中，有入侵者闯入或者试图闯入他们的企业网络。大部分专家都认为，大多数网络入侵活动都没有被检测出来。

交换机内集成的高性能防火墙模块

FWSM 安装在 Cisco Catalyst 6500 系列交换机或者 Cisco 7600 互联网路由器的内部，让这些设备的任何端口都可以充当防火墙端口，并且在网络基础设施中集成了状态防火墙安全。对于那些机架空间非常有限的系统来说，这种功能非常重要。

适应未来需要

FWSM 可以支持 5Gb 的吞吐量，因而可以提供无以伦比的性能，让用户无须对系统进行彻底的升级，就可以满足未来的要求。在 Catalyst 6500 中最多可以添加三个 FWSM，以满足用户不断发展的需求。

可靠性

FWSM 建立在 Cisco PIX 技术的基础之上，并使用了同一个经过时间检验的 Cisco PIX 操作系统——一个安全的、实时的操作系统。FWSM 可以利用行之有效的 Cisco PIX 技术检测分组，从而可以在同一个平台上提供性能和安全的独特组合。

低廉的整体运营成本

FWSM 可以提供所有防火墙中最佳的性能价格比。Cisco Catalyst 机型的 SmartNet? 合同中包含了维护成本。由于 FWSM 是基于 Cisco PIX 防火墙的，所以培训和管理成本都很低，而且由于它是集成在设备内部的，所以大大减少了需要管理的设备的数量。

易用性

Cisco PIX 设备管理器的直观的图形化用户界面（GUI）可以用于管理和配置 FWSM。在配置和监控方面，FWSM 可以获得思科管理框架和 Cisco AVVID（集成化语音、视频和数据体系结构）合作伙伴的支持。

FWSM 部署

今天的企业不仅仅需要周边安全，还需要连接业务伙伴和提供园区安全区域，为企业中的各个部门提供安全服务。FWSM 可以通过让用户和管理员以不同的策略在企业中设立安全域，提供一种灵活、经济、基于性能的解决方案。

网络入侵检测和威胁响应

IDS不会取代防火墙或者其它安全设备，但它能够作为这些产品的有效补充，。防火墙的主要功能是根据站点安全策略控制对服务和主机的访问。如果批准了通往某台主机的服务或连接，防火墙就允许所有流量通过，而不会再检查许可流量的内容。例如，如果允许公共访问 DMZ 上的某台 Web 服务器，那么，防火墙就会批准对此 Web 服务器上的超文本传输协议（HTTP）端口上的所有连接请求，包括来自 HTTP 服务器的试图利用缓冲器溢出易损点的恶意流量。多数防火墙无法防止数据 / 内容驱动的袭击（例如缓冲器溢出），但 IDS 可以。不仅如此，一般情况下，防火墙还无法预防来自网络内容的袭击，或者从防火墙不保护的入口（例如远程接入服务器）进入环境的袭击。IDS 无需影响网络就可以监控来自内部及其它入口的行为。将 IDS 作为防火墙的补充可以显著增强安全保护能力。

思科的集成化网络安全解决方案让机构可以防止他们的联网业务资产受到威胁，提高入侵防范的效率。这些解决方案中包括第二代思科入侵检测系统（IDS）模块，即 IDSM-2，它可以用在广泛部署的 Cisco Catalyst 6500 系列设备上。Catalyst 6500 系列设备的装机量已经达到数十万台，它是包括防火墙、虚拟专用网（VPN）和入侵检测系统（IDS）服务在内的附加服务的理想平台。由于认识到这种方式的价值，思科推出了这个第二代模块，以便为那些寻求 IDS 攻击防范的客户提供独特的优势。

Cisco IDSM-2 可以提供下列特性和优点:

- 思科是唯一可以提供一个交换机内置IDS解决方案的厂商，这种解决方案可以通过VLAN访问控制列表（VACL）获取功能来提供对数据流的访问权限。VACL 可以支持无限个 VLAN。
- 通过被动的、综合的操作提供透明的操作。这种操作方式可以通过VACL 获取功能和交换机端口分析工具 / 远程 SPAN（RSPAN/SPAN）检测分组的复本，而且如果设备需要维护，因为它并不位于交换机转发路径上，因而它不会导致网络性能降低或者中断。
- 体积只占一个机架单元，在 Cisco Catalyst 设备中只占用一个插槽，从而使它成为能够有效地支持所有 Catalyst 设备（从有三个插槽的 Catalyst 6503 到这个系列中最大的设备）的平台，并让用户可以根据自己的需要，同时安装多个模块，为更多的 VLAN 和流量提供保护
- 每秒 500Mb（Mbps）的 IDS 检测能力可以提供高速的分组检查功能，让用户可以为各种类型的网络和流量提供更多的保护。
- 多种用于获取和响应的技术，包括 SPAN/RSPAN 和 VACL 获取功能，以及屏蔽和 TCP 重置功能，从而让用户可以监控不同的网段和流量，同时让产品可以采取及时的措施，以消除威胁
- 使用与曾获大奖的 Cisco IDS 网络设备相同的程序代码，让用户可以将单一的管理技术作为标准，并让安装、培训、操作和支持变得更加便捷，同时可以利用 Cisco IDS 的全面的攻击识别能力和特征库。
- 重要的管理技术（例如 Cisco VMS 2.1 安全产品包提供的支持，以及内置的 Cisco IDS 设备管理器（IDM）、IDS 事件浏览器（IEV）本地管理功能和 CLI 支持）让 IDSM-2 更加便于管理，更加善于检测和响应威胁，同时就潜在的攻击向管理人员发出警报。此外，这个新的产品还让管理人员可以更加方便地在范围广泛、多样化的网络上管理多个设备。

网络入侵检测系统（NIDS）正在成为任何重要的网络安全战略不可或缺的组成部分。但是 NIDS 技术也可能会矫枉过正。数量和规模迅速扩大的安全攻击每天会引发数千次警报，管理人员很容易就会困于其中。更糟糕的是，目前的入侵检测技术还不能解决两个非常关键的问题:

1. 攻击是否成功?
2. 可以对它采取什么措施?

尽管看起来很简单，但是即便是最先进的入侵检测技术在这两个问题面前也束手无策。

攻击是否成功?

一般的 NIDS 主要是通过监控网络流量防御攻击。这是一种提供大范围网络监控的有效途径，但是它缺乏针对被攻击系统的监控。NIDS在报告攻击时，那些因为袭击安全系统而遭到失败的攻击的严重程度与成功的攻击完全一样。

这个问题在发生警报风暴时表现得尤为明显，甚至在对企业的日常监控中也会暴露出来。NIDS 可以检测到针对多个主机的多个攻击。所有的攻击都是实实在在的，即使很多系统都没有受到任何影响。因为管理员的资源有限，他们必须决定调查哪些攻击。通常，他们选择调查的攻击都是失败的攻击，而那些成功的攻击可能会逃过他们的调查。这使得他们可能会忽视一些非常严重的威胁。

可以对它们采取什么措施?

因为管理员的大部分时间通常都用于调查错误的警报（由失败的攻击产生的警报），因而他们很少有机会针对真实的威胁采取措施。在一个成功的攻击被发现之前，被攻击的系统上的一些关键罪证可能已经发生了变化，从而使得管理员难以成功地针对攻击事件采取措施。

思科威胁响应技术（CTR）提供了解决方案

利用关注于被攻击主机的创新入侵调查流程，集成了威胁响应技术的思科入侵检测系统可以准确地判断一个NIDS警报是否需要您的关注。领先的突发事件响应培训中心，包括SANS（系统安全、审核、网络、安全）协会和计算机安全协会（CSI）都强调了对被攻击主机进行罪证调查的重要性，以确定是否发生过某种特定攻击。思科威胁响应技术可以利用这些理念，以一种可重复的、可预测的方式每天 24 小时提供自动的调查。

思科威胁响应技术并不是一种关联技术。它既不会将防火墙、路由器、入侵检测系统和其他系统的日志整合到一起，也不对您的网络设计做任何假设。相反，思科威胁响应技术只关注于调查攻击的对象。思科威胁响应技术采用了三个核心的设计理念：集中关注，无需事先了解网络结构，不使用远程代理。

集中关注

思科威胁响应技术专门监控您的 NIDS 和对每个攻击进行全面的调查。因为思科威胁响应技术只关注于 NIDS 警报，所以它可以最准确、最全面地降低警报数量。思科威胁响应技术的设计理念是完全自动的调查和罪证分析。

无需事先了解网络结构

除了需要保护的IP地址的范围以外，使用思科威胁响应技术时不需要事先了解您的网络架构。现代网络通常都是动态变化的实体，经常需要添加、移除和更改其中的设备。只有在攻击者向您的某个系统发动攻击之后，思科威胁响应技术才需要了解您的系统的结构。通过进行这种定时的分析，思科威胁响应技术可以避免中断性的安全扫描，这通常会影响重要的网络服务。一种内置的缓存机制会实时地存储相关的攻击和对象信息——这有助于确保思科威胁响应技术在不对网络产生过度影响地情况下迅速做出反应。

不使用远程代理

与很多基于主机的入侵检测系统（HIDS）不同，思科威胁响应技术并不需要在它要保护的系统上安装远程代理。思科威胁响应技术只需使用现有的身份认证基础设施来自动完成所有调查响应。这种功能有助于最大限度地降低部署成本和防止可能存在不兼容问题的第三方代理影响网络系统。所有系统都享有相同级别的保护，无论它们在何时何地以何种方式加入。

威胁响应技术的工作流程

目前攻击者可以利用数以千计的漏洞攻击计算机系统。针对每个攻击都需要设置一种不同的调查和响应步骤。随时更新这些信息所需要的工作量非常惊人，即使对于安全专家来说也是如此。思科威胁响应技术产品使用了一套范围广泛的、预先定义的调查步骤，以确保迅速地分析每个检测到的攻击。

多阶段分析

思科威胁响应技术可以按照一个有经验的安全管理员的方式调查警报。当思科威胁响应技术收到警报时，它会启动一个多阶段分析流程，判断某个攻击失败或者成功。

1. **目标操作系统或者设备的弱点**——思科威胁响应技术可以迅速派遣一个代理，由它实时地判断运行在目标系统上的操作系统的运行状况。根据这些信息，思科威胁响应技术可以确定目标平台是否容易受到攻击。
2. **补丁级别检查**——思科威胁响应技术将全面地检查系统，了解是否安装了必要的补丁，以防止出现已被检测到的攻击。
3. **详细的系统调查**——思科威胁响应技术使用读写权限来根据攻击类型进行详细的系统调查。调查可能包括:
   - 分析注册表条目、系统和日志文件
   - 搜索特定文件或者目录，查找攻击的痕迹
   - 其他有助于判断攻击成功与否的调查方法
4. **搜集罪证**——如果确认发生了攻击，思科威胁响应技术将迅速地采取行动来搜集罪证，并将这些信息复制到某个安全的地点，以便进行离线分析和防止被篡改。
5. **确认攻击通知**——思科威胁响应技术将会向系统管理员发出警报，并提供关于攻击特征的信息、所进行调查的所有细节和所搜集的罪证的复本。

下面是两个可以证明思科威胁响应技术的作用的示例。第一个介绍了在没有思科威胁响应技术的情况下怎样处理一个常见的安全攻击（如图1所示），第二个介绍了怎样利用思科威胁响应技术处理同一个攻击（如图2所示）。这两个示例中使用的安全攻击都是一种IIS Unicode攻击，由Nimda蠕虫病毒传播，针对的对象是Microsoft IIS服务器。

图7
没有利用思科威胁响应技术防范入侵

一个攻击者启用了一个自动扫描脚本，在您的网络中搜索一种常见的Microsoft Unicode漏洞。很多攻击进入网络周边。

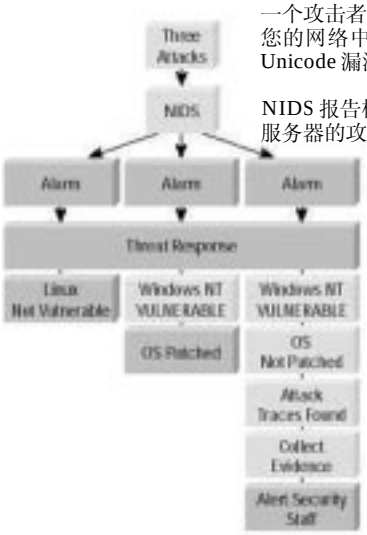
NIDS报告检测到很多针对您的网络中的服务器的攻击。

安全管理员在他们的NIDS和相关界面中看到很多攻击事件。他们将大量的时间用于调查每一次攻击。

对每个警报进行人工调查需要耗时15分钟：总共耗时：45分钟

在图7中，NIDS检测到大量可能发生的攻击。必须牢记的是，这些攻击都是实实在在的。在一个大型企业中，管理员可能会在很短的时间里面临数百个这样的攻击。数量有限的安全人员应当怎样分配他们的时间？如果只使用NIDS，他们将很难将成功的攻击与失败的攻击区分开来。IT安全人员必须人工调查每个警报，以确保企业的安全。（或者，他们可以选择部分警报进行调查，但是他们可能会选择错误的警报，这样企业的安全仍然会受到威胁。）最后，IT人员无法迅速有效地对实际的攻击做出反应。

图 8
利用思科威胁响应技术防范入侵



一个攻击者启用了一个自动扫描脚本，在您的网络中搜索一种常见的 Microsoft Unicode 漏洞。很多攻击进入网络周边。

NIDS 报告检测到很多针对您的网络中的服务器的攻击。

警报迅速地在威胁响应系统中排序以便分析。在无需预知网络状况或者安装远程代理软件的情况下可以实时地评估系统。

对成功的 IIS Unicode 攻击的调查步骤

1. 攻击是否针对这种 OS?
2. 是否安装了针对这种攻击的 OS 补丁?
3. 是否存在攻击成功的证据?
4. 复制罪证并将其存放在安全的地方。
5. 报告管理员发生了一个实际的、已得到确认的攻击

总耗时：5 秒

图8显示了思科威胁响应技术如何针对同一组事件提供一种智能化的入侵响应功能。NIDS可以检测到这些可能发生的攻击，并发出三个警报。思科威胁响应技术将收到这些警报，并立即开始对各个系统的实时调查:

系统 1：Linux 主机
- 进行一次检查，判断被攻击系统的操作系统。
  - 攻击是否针对操作系统？ – 不是。
- 降级警报。

系统 2：Windows NT 主机（已安装补丁）
- 进行一次检查，判断被攻击系统的操作系统。
  - 攻击是否针对操作系统？ – 是。
- 登陆该主机，检查是否已经安装了必要的服务包和补丁。
  系统是否安装了针对这种攻击的补丁？—是。
- 降级警报。

系统 3：Windows NT 主机（未安装补丁）
- 进行一次检查，判断被攻击系统的操作系统。
  - 攻击是否针对操作系统？ – 是。
- 登陆该主机，检查是否已经安装了必要的服务包和补丁。
  - 系统是否安装了针对这种攻击的补丁？—没有。
- 检查相关的 Web 服务器日志，查找成功的攻击的踪迹。
  - 是否找到了成功攻击的踪迹？——是的。
- 将所搜集的罪证复制到中央的命令控制服务器。
- 将攻击升级到紧急状态，促使管理员立即对其做出响应。

在不到五秒钟的时间里，思科威胁响应技术能够调查这些警报，判断哪个攻击获得了成功。为了迅速地找出问题，思科威胁响应技术还会在某个入侵者危及信息安全之前，从被攻击系统获取证据数据（例如日志文件）。

结论

在监控现代 NIDS 时，必须要记住什么是最关键的问题:

1. 攻击是否成功?
2. 可以对它采取什么措施?

思科威胁响应技术可以全面地回答这两个问题并帮助管理员实时、主动地调查和处理安全事件。思科威胁响应技术可以充当一个经验丰富的安全分析人员的眼睛，检查和分析各种警报，以便在不影响正常服务的情况下，迅速有效地发现和隔离您的企业所受到的攻击。它可以保护关键的证据，同时让管理员将有限的资源集中用于迫切的、需要立即消除的威胁上。总而言之，部署采用了思科威胁响应技术的思科入侵检测系统可以帮助企业保护他们的联网业务资产免受威胁，提高入侵防范系统的工作效率。

互连网内容访问管理

另外随着互连网开放性的发展，在获取越来越多的及时有效信息同时，大量无用或与工作无关的、非法的、色情的、危害网络安全的信息也在传播，成为校园网的新安全隐患。思科提供了内容管理引擎(Content Engine)硬件平台实现互联网访问管理。

Cisco Content Engine (缓存软件)具有以下优点:

- WAN 带宽节约 / 可扩展性
- 加快内容交付，提高员工工作效率
- 屏蔽网络中的有害信息 / 与业务无关的内容
- 服务器加速

图 9
内容管理引擎 CE 的工作示意图

透明缓存

Cisco Content Engine可以透明地缓存用户经常访问的内容，然后在当地满足用户的内容请求 而无需通过互联网/Intranet从远端的服务器库中获取内容，Cisco Content Engine可以最大限度地减少WAN链路上传输的多余网络业务。这样，服务供应商就可以迅速降低WAN 带宽成本，增加网络容量，以支持更多用户业务量及新业务，如话音业务。一般情况下，它可以节约 25%~60% 的带宽。

实时流媒体分割

Cisco Content Engine 可以从 WAN 中获取实时信息流，然后通过单点发送或组播发给多个下行用户，最大限度地提高 WAN 带宽的可扩展性 。

反向代理缓存

此外，Cisco Content Engine 还可以部署在 Web 站点之前，以便大幅度提高服务器性能。通过缓存或分离入局的内容请求, 这些内容引擎还可以大幅度减少来自原始服务器的业务量及 TCP连接数量。

内容过滤

与 Smartfilter 企业软件或者配合思科网络产品针对校园开发《大拇指互联网管理系统——校园增强版》协同运行时，Cisco Content Engine 使系统管理员可以监控、管理学生对与业务无关的或有害内容的访问并进行报告。这样可以提高员工的工作效率、降低带宽使用量并减轻法律责任。

安全管理特殊需求分析

由于校园网络当中常见一些非法的规避行为，例如私设代理服务器、手工设置 IP 地址等，从而实现多台 PC 共享一个包月接入等逃避计费目的。目前我们考虑的解决方案包括:

多台 PC 共享一个包月接入等逃避计费、私设代理服务器

1、采用 802.1x 技术之后，可以做到用户必须经过认证才可访问网络，故而可以解决通过更改 IP/MAC 地址逃避计费的问题;

2、带端口安全性的 802.1 X 分为三种认证模式:

- 单认证模式(single-authentication)
- 多用户模式(multiple-host)
- 多认证模式(multiple-authentication modes).

在普通情况下一个交换机端口只接一个用户采用单认证模式。在交换机端口下接有Hub的情况，可以采用多用户模式和多认证模式; 在多用户模式的情况时，所有接在 Hub 下的用户只要有一个通过认证其他都不需要认证就可以进行通信; 在多认证模式的情况下，所有在 Hub 下的用户都要单独进行认证，在这种状态下，所有用户可以单独根据用户名和密码进行认证和计费。Cisco 每台交换机的端口安全支持 132 个 MAC 地址。

3、我们主要需要解决的是多台共享包月的问题。一方面做到单一用户网络访问唯一性，即一个用户在某一时刻只可在一点接入; 另一方面，在单一用户访问网络时，通过 802.1x 中心认证服务器向交换机发送流量限制的参数。思科核心交换机可以实现准确限速（CAR），例如 512Kbps/用户。这样可以减少多用户共享包月对网络造成的不良影响。现在比较推荐的方式还有加载客户端驻留程序，如“城市热点”提供的防代理程序。

私设 DHCP 服务器

通过思科交换机提供的 DHCP 中继（DHCP Relay）和 DHCP 侦听（DHCP Snooping）来将正常 DHCP 服务请求跨越不同 VLAN 中继到网络中事先设定的 DHCP 服务器。而不合法的 DHCP 服务器，交换机侦听到其服务信息时将自动屏蔽该端口。

手工设置 IP 地址

首先在校园网中推荐的方式是，服务器尤其是核心应用服务器设置固定 IP 地址，并设置在特定网段和 VLAN 中。学生或一般教工用机通过 DHCP 分配 IP 地址，此 IP 地址需要绑定 MAC 地址（预先设置好在 DHCP 服务器和 AAA 服务器中），并且划归为与服务器网段不同的网段，不同的 VLAN。

如果有学生或教工私自手工设置IP地址，

- 设置与服务器一样的IP，由于网段和VLAN不同，二层交换机不具备路由功能，将限制此客户机的访问
- 设置为同一网段中其他用户IP地址，如果两个相同IP的客户机在线将无法做任何网络资源访问，可以用网络管理和网络分析设备发现；合法IP地址的用户退出网络，服务选择网关（SSG）会设时限时将此IP会话结束，如果盗用IP地址的客户机单独上网，服务选择网关（SSG）将此机器的服务申请转到AAA服务器要求再次进行身份认证。
- 如果客户机同时盗用IP地址和MAC地址，他也必须通过SSG进行用户名和密码验证。网络资源的使用和收费是基于用户身份认证来实现，不是按照IP地址和MAC地址来实现。每种服务（国内、国外网络访问，FTP，视频点播，数据库，电子邮件等等）都可以按需要要求用户验证。用户的密码可以在AAA服务器中要求强制定期更新，如3个月换一次。

攻击者为了不暴露身份，通常使用假IP地址，使被攻击者无法追踪。

这时可以使用RFC2827过滤（逆向源地址路由检查－uRPF），思科7301路由器IOS具备这个功能，需要在配置时启用。路由器对入口IP包的源IP地址查询路由表，如果没有相应回去的路由，则判断为伪地址包，从而丢弃。

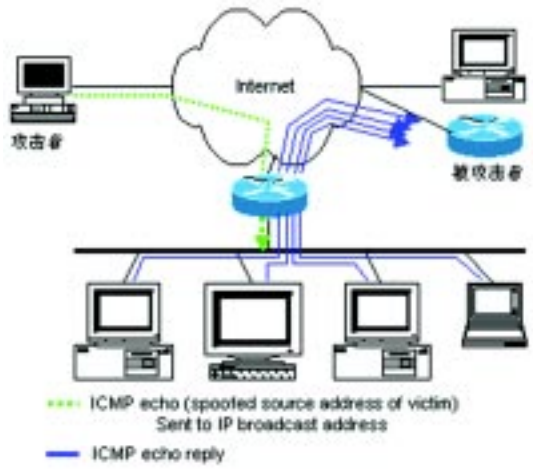
防止私有地址、SQL 蠕虫攻击

可以使用ACL对私有地址数据包过滤－RFC1918过滤在核心交换机的端口配置ACL,丢弃源地址为私有IP地址的数据包对于SQL蠕虫攻击，可以采用ACL屏蔽UDP端口为1434的数据包。

对于 ICMP 攻击的防范

攻击者可以利用合法的网络协议ICMP，通过向被攻击设备（主机、路由器的端口）发出大量的Ping包(ICMP-echo)，消耗被攻击设备资源(如CPU)，使其无法正常工作。其中一种攻击(smurf)如图10所示:

图10
防止伪地址攻击



可以利用思科核心设备准确限速（CAR）功能对ICMP流量进行限制，丢弃大量无用的ICMP流量；屏蔽ICMP Unreachable，ICMP redirect流量；避免成为Smurf攻击流的反射器（reflector）。

思科解决方案特点

更安全的网络核心平台

对于校园网而言，应用种类繁多，如网上点播、网络远程教学、网络电视会议、网上备课、资源共享、E-mail、FTP、网络论坛、网络图书馆、搜索引擎、IP 电话等。要实现复杂的应用通过网络流畅地传输，并且实现网络管理的统一性，需要选择不仅具有：高性能、高可用性、安全可扩展的产品，更需要关注厂商的生存能力、售后服务以及是否能提供完整的端到端的解决方案。

产品性能

在众多独立测试中显示，Catalyst 系列交换机在大的网络流量，大的路由数量，以及使用大量的安全、QoS 策略的情况下，运行非常稳定，丢包率极低，远远优于其它同类产品。这主要来自思科 IOS 软件经过多年的改进以及市场的长期考验。Catalyst 6500 支持 720Gbps 背板、400Mpps 包转发能力,(或 256Gbps 背板、210Mpps 包转发能力)，支持 64000 条 ACL。Catalyst 4500 支持 64Gbps 背板、48Mpps 包转发能力，支持 32000 条 ACL。

思科公司拥有专利的 CEF（Cisco Express Forwarding）技术，可以避免对第一个数据包的慢速交换，从而实现更快速的交换，提升设备对大型网络、复杂应用网络的处理能力。(目前市场上大部分交换机的转发机制为 Flow-based switching 或 Cache-based switching，必须对第一个数据包进行通过 CPU 的软件路由。随着网络中应用的演变，可以看到，今天网络中的流量大部分情况下，为更换频繁的短小的数据流，所以不得不对第一个数据包进行处理的 flow-based/cache-based switching 机制就会导致性能下降。而 CEF 技术，采用 FIB（Forwarding Information Base），避免对第一个数据包的处理，保证性能不会随流量的变化而下降。即使是在思科的中低端产品上，思科也非常注意性能的保证。例如，在 Catalyst 3550 上也支持 CEF 技术，从而实现通过思科网络设备构建的网络由于优越的性能。

这种 CEF 交换技术在网络流量负载大，会话数量多的情况下尤其得心应手。甚至在发生蠕虫病毒的情况下，普通三层交换机会因为会话数量急遽增加，造成中心处理器的负载无法承受，从而导致网络瘫痪。但是，CEF 交换不会因为会话数量的增加而加大机器处理能力的负载，故而仍可以正常工作。这种特性在多次病毒大爆发的情况下，已经得到全球思科用户的确认，可以大大增强网络的可用性。在 Catalyst 系列交换机上，通过硬件 TCAM 的方式实现安全功能、QoS 功能、组播功能。流量即使增加了，性能也不会下降。适用于校园网复杂的应用环境。

稳定性、高可用性

- 设备的高可用性

思科的交换机使用无源背板，以提高设备的稳定性。另外，对于关键模块都采用冗余设计，如冗余的交换背板、冗余的时钟模块、冗余的引擎（管理模块）、冗余的电源、冗余的风扇等，从而实现无论是用户易见的还是不易见的模块都不影响设备的可用性。

- 网络的高可用性

通过设备和链路的冗余设计、三层（路由）网络的设计提高网络的可靠性。而这些可靠性，依靠以下关键技术实现：在二层协议方面支持 STP（Spanning Tree protocol）、Enhanced STP(Uplink fast & Backbone fast & Port fast)以及 802.1s/802.1w 等协议，实现二层链路的切换由原来的 30 秒钟降低到 2 秒种再降低到 1 秒钟以内，从而保证二层链路的快速切换;

在接入层交换机后，网络的互联采用路由技术，通过路由的快速收敛能力实现大型网络的高可用性。思科自 1984 年生产第一台路由器以来，在路由方面以快速、稳定、大型网络应用经验而著称，其核心的 IOS 软件经过大量用户的长期考验，得到市场的充分认可。目前，Internet 上 80%的流量通过思科的设备传输；财富 500 强中，90%的用户选用思科公司的产品。在国内大型服务供应商、银行、证券、保险、政府、教育、医疗等行业的骨干网络都是选用思科公司的产品。

构筑安全与智能的校园网体系——思科校园网络安全解决方案

安全性

思科充分认识到安全对用户的重要性，在端到端的解决方案中，提供完整的安全方案，包括用户认证、防火墙边界安全、入侵检测、VPN 虚拟专网、统一的安全管理。

对内

在思科Catalyst 6509交换机上，可以使用业界最高性能的防火墙模块，入侵检测模块，从而实现网络内部的安全保护。思科公司还提供软件、硬件安全产品，如PIX系列防火墙可以保护内部网络及服务器的安全；IDS Sensor入侵检测产品可以预警网络受到的攻击；Cisco Scanner漏洞扫描产品可以预先检查网络中、服务器中的安全漏洞；思科交换机中的IOS安全软件也可以提供灵活的防火墙、入侵检测等安全解决方案。所有这些产品，与思科公司的网络产品接合起来，可以实现良好的互动性，从而提高网络的安全设计。

对外

在思科Catalyst 6509交换机上的防火墙模块，入侵检测模块和VPN模块可以实现网络外部的安全保护。思科公司还提供软件、硬件安全产品，如PIX系列防火墙可以构建安全边界；IDS Sensor入侵检测产品可以预警网络受到的攻击；思科交换机中、路由器中的IOS安全软件也可以提供灵活的防火墙、入侵检测等安全解决方案。

所有这些产品，与思科公司的网络产品接合起来，可以实现良好的互动性，从而提高网络的安全设计。

帐号管理

思科公司的用户管理可以通过AAA软件：CiscoSecure ACS实现，该软件提供AAA功能，并且支持2个服务器的备份工作方式，从而提供可靠性。CiscoSecure ACS软件支持NT数据库用户数据的导入，降低工作量。

CiscoSecure ACS支持有线用户和无线用户的认证，也支持网管人员对网络设备配置的授权功能，如可以对不同权限用户授予不同的访问能力，有的用户可以配置网络设备，有的用户只可以查看配置，不能更改，甚至可以设置什么样的用户可以使用什么样的命令。

思科服务选择网关（SSG）

为配合802.1X的应用，思科的7301特殊应用路由器还提供了针对不具备802.1X技术的设备进行基于身份的网络服务，即服务选择网关（Service Selection Gateway）。与SSG一道，服务选择面板（SSD）允许服务供应商创建受控门户，在这个门户中用户可以使用一个Web浏览器选择服务。受控门户使网络运营和管理者能够为服务作广告、创建自己的特色网络应用服务并获得用户体验。

服务自选网关（SSG）实际上是一个终结用户接入的设备和AAA功能的一个集合。Cisco SSG实现了基于Radius的计费和认证系统，支持Bridged、PPPOE、PPPOA等服务以及基于WEB的SSD(现为SESM)的应用；在组播支持、基于用户过滤等方面能够实现集中或分布式的应用方式。另外，第二层、第三层服务的选择、服务定制、服务列表的定义等问题，都很容易解决。

CiscoSSD/SSG解决方案适用于校园园区、居民区以及楼宇网络的用户控制、服务选择和记账。它能够为用户提供基于WEB的服务选择的界面，让用户能够同时享受多种服务；对于运营商而言SSD/SSG能够对每个用户的每次网络访问分别记账，并且支持Radius多种标准属性，可以实现对用户访问的基于“流量”的记账（当然也支持基于“时长”的记账方式）。

CiscoSSD/SSG 方案包括三个组成部件：SSD、SSG 和 AAA 服务器。

SSG (Service Selectiong Gateway)

基于 Cisco7400 或者是 Cisco7300 硬件平台的“服务选择网关”，它的功能是执行管理员设置的对用户的“任务”管理的策略（7400/7300 时通过 IP 层的路由控制来达到对用户的网络访问行为进行控制的）。

如下图显示的 SSG 工作原理：

图 11
SSG 工作原理

SSD (Service Selection Dashboard)

安装在 UNIX 或者是 NT 平台上的基于 JAVA 的 Web 服务器，提供给最终用户做“自助式”的服务选择。SSD 作为服务选择解决方案的一部分，主要功能对 SSG 进行控制，为终端用户提供:

- 通过 SSG 连接到相应的服务的接口;
- 查看联接的状态，包括“当前状态（通、断）”、“连接的时长”等。
- 查看系统日志信息（用户连接 SSG 的历史纪录）。

AAA(Authentication/Authoration/Accounting) 服务器

安装在 UNIX 或者是 NT 平台上的用于执行“认证、授权、记账”的 Radius 软件， 在 AAA 服务器中，我们可以为每一个用户或一组用户定义其所能够访问的网络，从而控制每个用户或者是一组用户的网络访问行为; 同时 AAA 服务器也是计帐数据的采集器，能够生成基于每个用户的每一次“任务”（一次对网络的访问）生成独立的计帐信息。作为最终提交给计费系统的原始数据。所生成的数据是标准的 Radius 记账数据，提供“任务”的“开始时间”、“结束时间”、“任务时长”等一些的记账信息。同时，在 AAA 服务器中，可以通过对用户数据的配置，决定用户对网络的访问的权限，同时对用户上网访问不同服务的控制，以及控制上网的时长（可以通过使用“Session-Timeout”、“Idel-Timeout”等 Radius Attribute 来对用户的任务进行控制）。

工作过程描述

用户通过以太网交换机联接到校园网络中，由于采用SSG/SSD的方式来控制用户行为，在用户身份认证之前，没有任何路由信息，即，不能访问Internet或是校园网络内部的任何需要收费的内容（当然，校园网络也可以根据自己的网络运营的需要，自行设计用户访问控制策略，可以做到所有的用户不需要认证过程，开放所有的服务，用户使用的任何一种服务都将被记账）。

SSD（安装在UNIX或者是NT平台上的Web服务的软件）会以web的方式给用户提供服务界面，让用户自己选择希望得到的服务，同时，服务提供商能够根据不同用户的类型把用户分类，通过密码认证的方式来区分不同种类的用户；在不同类型的用户所看到的web上，是有着不同的服务图标供用户自己选择。

用户可以根据自己的喜好和需求选择服务（如WWW、E-mail、FTP、VOD等等，点击代表该服务的图标），在列表中个被选中的服务的图标会自动改变颜色，成为激活的状态。这时就可以使用该服务。SSG会实时的把用户的“任务”与对应所选择的服务的“路由”进行“绑定”，从而使用户的主机能够访问到“服务”所在的网络的IP地址。

用户即使已经连通网络，但是在没有申请服务之前，是不计帐的；在用户点击服务图标，确认服务后，SSG会以标准的Radius的格式对（用户，服务）进行计帐，如果用户同时享受多种服务，在计帐信息中是各自孤立单独记帐的。同时，用户在自己的客户端web上能够实时的看到自己正在享受的服务的时长，这样用户就能够灵活的掌握服务的使用了。服务商为用户提供的服务，是事先在Radius中，以用户数据信息的形式存储在Radius Server中的。

校园网络运营者可以根据自己的经营策略以及所能够提供的服务，与用户签订服务协议，从而规定给用户所能够享受的服务，以及各项的服务价格，最终体现在给用户访问SSD时说看到的web界面上显示的服务的图标。每个校园网络中的用户在发出各项应用申请时，SSG设备（CISCO7301）能为针对不同IP目的地的用户交互策略提供RADIUS身份认证和记帐功能，并允许用户按照自己的需要动态地选择服务。然后，SSG会将用户通信流切换到所选择的服务，并在这一过程中实施全面的边界路由选择和服务质量（QoS）策略。

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)85155000
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)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

欢迎下载电子文档，http://www.cisco.com/cn/power/industry/edu/index.shtml

2005 年 3 月印刷