3

医疗级网络安全保障
解决方案

三． 医疗级网络安全保障解决方案

3.1 医院网络安全现状及挑战

现阶段，医院信息系统正在变成医疗体系结构中不可或缺的基础架构。该架构的网络安全和数据可用性变得异常重要。任何的网络不可达或数据丢失轻则降低患者的满意度，影响医院的信誉，重则引起医患纠纷、法律问题或社会问题。和其它行业的信息系统一样，医疗信息系统在日常运行中面临各种安全风险带来的安全应用事故。

各医院在网络和应用系统保护方面分别采取了很多安全措施，例如在每个网络、应用系统分别部署了防火墙、访问控制设备，采取了备份、负载均衡、硬件冗余等安全措施；也可能实现了区域性的集中防病毒，实现了病毒库的升级和防病毒客户端的监控和管理；采用系统账号管理、防病毒等方面具有一定流程。但在网络安全管理方面的流程相对比较薄弱，需要进一步进行加强；另外主要业务应用人员安全意识有待加强，日常业务处理中存在一定非安全操作情况，终端使用和接入情况复杂。这可以说是现阶段具有代表性的网络安全建设和使用的现状，不仅仅是在医院。从另一个角度来看，单纯依靠网络安全技术的革新，不可能完全解决网络安全的隐患，很难从根本上克服网络安全问题，我们首先来分析目前医院网络环境所面临的安全威胁究竟是什么，这也是我们最关心的安全问题：

- 网络安全管理体系不完善，需要通过实施策略对流程进行细化，其它体系也需要按照网络安全管理体系和流程要求不断完善其内容。
- 在物理与环境安全、系统和网络安全管理、系统接入控制方面仍然存在一定差距，在安全策略、安全组织、人员管理、资产分类控制、安全审计方面存在明显不足。
- 防病毒系统没有实现整体统一，存在防病毒的局部能力不足。
- 历史原因造成网络自身安全防护不足，大量的第二层的攻击（如MAC地址泛洪、DHCP服务器欺骗、ARP欺骗、IP/MAC欺骗）让网络失效或者通过获取诸如密码这样的敏感信息而危及网络用户的安全。而传统的IP/MAC/Port绑定技术复杂而且效率较低。
- 没有部署针对服务器/主机的安全保护，而大量的基于Web的应用导致病毒或非法攻击，甚至于非法copy等，无法保护业务数据的安全。而针对医院来说，业务数据就是核心，这点尤其重要。
- 网络、应用系统防护上虽然采取了防火墙等安全产品和硬件冗余等安全措施，但安全产品之间无法实现联动，安全信息无法挖掘，安全防护效果低，投资重复，存在一定程度的安全孤岛现象。另外，安全产品部署不均衡，各个系统部署了多个安全产品，但在系统边界存在安全空白，没有形成纵深的安全防护。
- 对终端管理没有统一策略，操作系统版本、操作系统补丁等没有统一的标准和管理。
- 没有应急响应流程和业务持续性计划，发生安全事件后的处理和恢复流程不足，对可能造成的业务中断没有紧急预案。

综上所述，网络安全问题越演越烈，不仅仅是一个单独的设备能防御，在技术上也陷入了被动应付的局面。思科自防御网络的出现，为医院网络安全提供了由低级到高级不断发展、演进的解决方案。思科网络设备集成了独特的安全功能，以及各个安全设备的联动并主动进行防护，是思科自防御网络的具体实现。

思科自防御网络的构想起源于“人体”，其目标是让IT基础设施和网络像“活”的系统一样运行。在人所处的环境中，病毒是永远存在的不争事实，我们携带着病毒，我们从各种接触中感染病毒。人体虽然携带着病毒和病原体，但人体机能仍可正常运行，因为人具有自体免疫功能。自体免疫概念就是思科安全构想与战略的构建基础。

3.2 思科自防御网络安全系统

随着新一代安全威胁和安全需求的出现，思科提出了自防御网络安全战略，它标志着整个网络安全架构的巨大变革，从过去的反应式防御迈向自动识别、自适应、主动防御。思科自防御网络安全是一个全面的战略，需要多阶段实施，逐步完善。目前已经有三个阶段：
集成式安全、协作式安全、自适应威胁防御。

思科自防御网络战略的蓝图如下图所示。通过端点安全、设备安全、动态连接、动态通讯、自动响应等方面的创新，实现安全连接、威胁防御、信任识别和安全管理，实现的手段包括网络准入控制、安全运营管理、安全自动响应和安全专业服务等几个层面的内容。

安全实现。实现思科自防御网络，提供具体完整的、可实施、可管理的、集成模块化自防御网络解决方案，主要包含几大部分：安全的连接保证，身份信任与识别确认，自适应威胁防御，智能化安全管理。

安全创新。安全技术创新是思科自防御网络的基础，将带领思科自防御网络稳步走向未来。创新的安全技术包括多个领域：终端安全技术，设备安全技术，自动响应技术，动态安全连接技术，智能化安全管理等方面。

系统安全。自防御网络除了安全技术创新的支撑，还需要系统化的安全体系架构，其主要包括两方面的含义：网络的不同部分，共同协作，构成一个完整的安全系统；多方的安全联盟共同提供面向不同层面、不同应用的全面安全解决方案。

（图）思科自防御网络：实现IT信息安全的系统方法

针对于医院园区网络，下图概括了整个园区的网络安全所涉及的区域及解决方案。

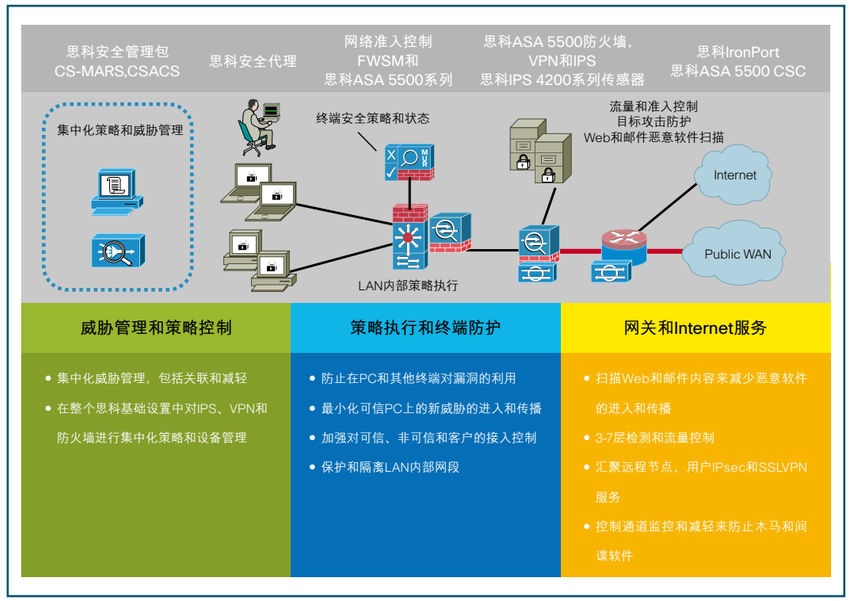
1. 构建安全的基础网络平台

在诸多的局域网安全问题中，由于历史原因，令网络管理员感到最头痛的问题就是IP地址的管理；最担心的问题就是账号、密码的盗取以及信息的失窃和篡改；而最棘手的问题就是木马、蠕虫病毒爆发对网络造成的危害。据CSI/FBI计算机犯罪与安全调查显示，信息失窃已经成为当前最主要的犯罪。在造成经济损失的所有攻击中，有75%都是来自于园区内部。这样，企业网络内部就必须采用更多创新方式来防止攻击，如果我们将网络中的所有端口看成潜在敌对实体获取通道的“端口防线”，网络管理员就必须知道这些潜在威胁都有那些，以及需要设置哪些安全功能来锁定这些端口并防止这些潜在的来自网络第二层的安全攻击。

网络第二层的攻击是网络安全攻击者最容易实施，也是最不容易被发现的安全威胁，它的目标是让网络失效或者通过获取诸如密码这样的敏感信息而危及网络用户的安全。因为任何一个合法用户都能获取一个以太网端口的访问权限，这些用户都有可能成为黑客，同时由于设计OSI模型的时候，允许不同通信层在相互不了解情况下也能进行工作，所以第二层的安全就变得至关重要。如果这一层受到黑客的攻击，网络安全将受到严重威胁，而且其他层之间的通信还会继续进行，同时任何用户都不会感觉到攻击已经危及应用层的信息安全。

所以，仅仅基于认证（如IEEE 802.1x）和访问控制列表（ACL，Access Control Lists）的安全措施是无法防止来自网络第二层的安全攻击。一个经过认证的用户仍然可以有恶意，并可以很容易地执行本文提到的所有攻击。目前这类攻击和欺骗工具已经非常成熟和易用。

（图）医院园区中的自防御网络



以上所提到的攻击和欺骗行为主要来自网络的第二层。在网络实际环境中，其来源可概括为两个途径：人为实施，病毒或蠕虫。人为实施通常是指使用一些黑客的工具对网络进行扫描和嗅探，获取管理帐户和相关密码，在网络上中安插木马，从而进行进一步窃取机密文件。攻击和欺骗过程往往比较隐蔽和安静，但对于信息安全要求高的企业危害是极大的。木马、蠕虫病毒的攻击不仅仅是攻击和欺骗，同时还会带来网络流量加大、设备CPU利用率过高、二层生成树环路、网络瘫痪等现象。

归纳前面提到的局域网目前普遍存在的安全问题，根据这些安全威胁的特征分析，这些攻击都来自于网络的第二层，主要包括以下几种:

- MAC地址泛滥攻击
- DHCP服务器欺骗攻击
- ARP欺骗
- IP/MAC地址欺骗

利用Cisco Catalyst交换机内部集成的安全特性，采用创新的方式在局域网上有效地进行IP的地址管理、阻止网络的攻击并减少病毒的危害。Cisco Catalyst 智能交换系列的创新特性针对这类攻击提供了全面的解决方案，将发生在网络第二层的攻击阻止在通往内部网的第一入口处，主要基于下面的几个关键的技术:

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard

我们可通过在思科交换机上组合运用和部署上述技术，从而防止在交换环境中的“中间人”攻击、MAC/CAM攻击、DHCP攻击、地址欺骗等，更具意义的是通过上面技术的部署可以简化地址管理，直接跟踪用户IP和对应的交换机端口，防止IP地址冲突。同时对于大多数具有地址扫描、欺骗等特征的病毒可以有效的报警和隔离。

通过启用端口安全功能，可有效防止MAC地址泛洪攻击，网络管理员也可以静态设置每个端口所允许连接的合法MAC地址，实现设备级的安全授权。动态端口安全则设置端口允许合法MAC地址的数目，并以一定时间内所学习到的地址作为合法MAC地址。

通过配置Port Security可以控制:

- 端口上最大可以通过的MAC地址数量
- 端口上学习或通过哪些MAC地址
- 对于超过规定数量的MAC处理进行违背处理

端口上学习或通过哪些MAC地址，可以通过静态手工定义，也可以在交换机自动学习。交换机动态学习端口MAC，直到指定的MAC地址数量，交换机关机后重新学习。目前较新的技术是Sticky Port Security，交换机将学到的MAC地址写到端口配置中，交换机重启后配置仍然存在。

对于超过规定数量的MAC处理进行处理一般有三种方式（针对交换机型号会有所不同）:

- Shutdown：端口关闭
- Protect：丢弃非法流量，不报警
- Restrict：丢弃非法流量，报警

Catalyst交换机可通过DHCP Snooping技术保证DHCP安全特性，通过建立和维护DHCP Snooping绑定表过滤不可信任的DHCP信息，这些信息是指来自不信任区域的DHCP信息。通过截取一个虚拟局域网内的DHCP信息，交换机可以在用户和DHCP服务器之间担任就像小型安全防火墙这样的角色，“DHCP监听”功能基于动态地址分配建立了一个DHCP绑定表，并将该表存贮在交换机里。在没有DHCP的环境中，如数据中心，绑定条目可能被静态定义，每个DHCP绑定条目包含客户端地址（一个静态地址或者一个从DHCP服务器上获取的地址）、客户端MAC地址、端口、VLAN ID、租借时间、绑定类型（静态的或者动态的）。

通过部署动态ARP检查（DAI，Dynamic ARP Inspection）来帮助保证接入交换机只传递“合法的”的ARP请求和应答信息。DHCP Snooping监听绑定表包括IP地址与MAC地址的绑定信息并将其与特定的交换机端口相关联，动态ARP检测（DAI－Dynamic ARP Inspection）可以用来检查所有非信任端口的ARP请求和应答(主动式ARP和非主动式ARP)，确保应答来自真正的ARP所有者。Catalyst交换机通过检查端口记录的DHCP绑定信息和ARP应答的IP地址决定是否真正的ARP所有者，不合法的ARP包将被删除。

DAI配置针对VLAN，对于同一VLAN内的接口可以开启DAI也可以关闭，如果ARP包从一个可信任的接口接收到，就不需要做任何检查，如果ARP包在一个不可信任的接口上接收到，该包就只能在绑定信息被证明合法的情况下才会被转发出去。这样，DHCP Snooping对于DAI来说也成为必不可少的，DAI是动态使用的，相连的客户端主机不需要进行任何设置上的改变。对于没有使用DHCP的服务器个别机器可以采用静态添加DHCP绑定表或ARP access-list实现。

另外，通过DAI可以控制某个端口的ARP请求报文频率。一旦ARP请求频率的频率超过预先设定的阈值，立即关闭该端口。该功能可以阻止网络扫描工具的使用，同时对有大量ARP报文特征的病毒或攻击也可以起到阻断作用。

除了ARP欺骗外，黑客经常使用的另一手法是IP地址欺骗。常见的欺骗种类有MAC欺骗、IP欺骗、IP/MAC欺骗，其目的一般为伪造身份或者获取针对IP/MAC的特权。Catalyst IP源地址保护（IP Source Guard）功能打开后，可以根据DHCP侦听记录的IP绑定表动态产生PVACL，强制来自此端口流量的源地址符合DHCP绑定表的记录，这样攻击者就无法通过假定一个合法用户的IP地址来实施攻击了，这个功能将只允许对拥有合法源地址的数据保进行转发，合法源地址是与IP地址绑定表保持一致的，它也是来源于DHCP Snooping绑定表。因此，DHCP Snooping功能对于这个功能的动态实现也是必不可少的，对于那些没有用到DHCP的网络环境来说，该绑定表也可以静态配置。

IP Source Guard不但可以配置成对IP地址的过滤也可以配置成对MAC地址的过滤，这样，就只有IP地址和MAC地址都于DHCP Snooping绑定表匹配的通信包才能够被允许传输。此时，必须将 IP源地址保护IP Source Guard与端口安全Port Security功能共同使用，并且需要DHCP服务器支持Option 82时，才可以抵御IP地址＋MAC地址的欺骗。

与DAI不同的是，DAI仅仅检查ARP报文， IP Source Guard对所有经过定义IP Source Guard检查的端口的报文都要检测源地址。

通过在交换机上配置IP Source Guard，可以过滤掉非法的IP/MAC地址，包含用户故意修改的和病毒、攻击等造成的。同时解决了IP地址冲突的问题。

以上所列的基础安全防护的功能，均内置在思科的Catalyst交换机内，无需另外购买。

2. 终端设备的安全接入管理及防护

病毒、蠕虫和间谍软件等新兴网络安全威胁继续损害医院利益。与此同时，移动计算的普及进一步加剧了威胁。移动用户能够从家里或公共热点连接互联网或医院网络——常在无意中轻易地感染病毒并将其带进医院环境，进而感染医院网络。医疗网络上的用户无意中感染病毒或蠕虫，可能影响全网的运行。通过网络准入控制(Network Admission Control, NAC)，可以检查用户终端是否安装了信息中心规定的安全软件及安全数据库，只有符合规定安全策略的终端才能连入医疗网络。

思科网络准入控制（NAC）方案可利用网络基础设施来防止病毒和蠕虫危害网络。使用Cisco NAC，各医院可完全依据已出台的安全策略来控制PC、PDA及服务器等端点设备对网络的访问。

Cisco NAC拒绝不符合要求的设备访问网络，将其放置在隔离区或限制其对计算资源的访问。Cisco NAC可防止新病毒入侵网络，解决环境的复杂性问题，同时提供超越点安全技术的优势。点安全技术只关注主机，而不是网络的全局可用性和医院的整体弹性。

从病毒和蠕虫造成的损害中可以看出，现有的安全解决方案不足以应对病毒和蠕虫的威胁。Cisco NAC是最新的全面解决方案，允许各医院实施主机补丁策略和病毒防范策略（与终端操作系统和防病毒），将不符合安全策略要求及可疑的系统放置到隔离环境中，限制或禁止其访问网络。通过将端点安全状态信息与网络准入控制的执行标准结合在一起，Cisco NAC使各机构能够大幅度提高其计算基础设施的安全性。

Cisco NAC允许符合安全要求的可信端点设备访问网络（如PC、服务器及PDA等），同时限制不符合安全策略要求的设备访问网络。访问决策可根据端点的防病毒状态及操作系统的补丁级别做出。

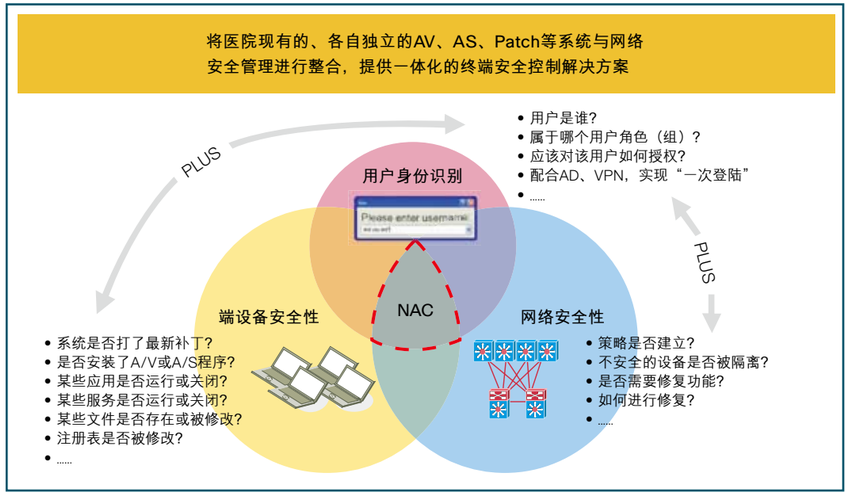
网络准入控制（NAC）进行了专门设计，可确保为访问网络资源的所有终端设备（如PC、笔记本电脑、服务器、智能电话或PDA等）提供足够保护，以防御网络安全威胁。

据CSI/FBI安全报告称，虽然安全技术多年来一直在发展且安全技术的实施更是耗资数百万美元，但病毒、蠕虫、间谍软件和其他形式的恶意软件仍然是各机构现在面临的主要问题。机构每年遭遇的大量安全事故造成系统中断、收入损失、数据损坏或毁坏以及生产率降低等问题，给机构带来了巨大的经济影响。

显然，仅凭传统的安全解决方案无法解决这些问题。思科系统公司开发出了将领先的防病毒、安全和管理解决方案结合在一起的全面的安全解决方案，以确保网络环境中的所有设备都符合安全策略。NAC允许您分析并控制试图访问网络的所有设备。通过确保每个终端设备都符合医院安全策略（例如运行最相关的、最先进的安全保护措施）机构可大幅度减少甚至是消除作为常见感染源或危害网络的终端设备的数量。

NAC是构建在思科系统公司领导的行业计划之上的一系列技术和解决方案。NAC使用网络基础设施对试图访问网络计算资源的所有设备执行安全策略检查，从而限制病毒、蠕虫和间谍软件等新兴安全威胁损害网络安全性。

（图）思科网络准入控制（NAC）策略



实施NAC的客户能够仅允许遵守安全策略的可信终端设备(PC、服务器及PDA等)访问网络，并控制不符合策略或不可管理的设备访问网络。

通过运行NAC，只要终端设备试图连接网络，网络访问设备(LAN、WAN、无线或远程访问设备)都将自动申请已安装的客户端或评估工具提供终端设备的安全资料。随后将这些资料信息与网络安全策略进行比较，并根据设备对这个策略的符合水平来决定如何处理网络访问请求。网络可以简单地准许或拒绝访问，也可通过将设备重新定向到某个网段来限制网络访问，从而避免暴露给潜在的安全漏洞。此外，网络还能隔离设备，它将不符合策略的设备重新定向到修补服务器中，以便通过组件更新使设备达到策略符合水平。

NAC执行的某些安全策略符合检查包括:

- 判断设备是否运行操作系统的授权版本。
- 通过检查来查看操作系统是否安装了适当补丁，或完成了最新的热修复。
- 判断设备是否安装了防病毒软件以及是否带有最新的系列签名文件。
- 确保已打开并正在运行防病毒技术。
- 判断是否已安装并正确配置了个人防火墙、入侵防御或其他桌面系统安全软件。

NAC随后根据上述问题的答案做出基于策略的明智的网络准入决策。

- 帮助确保所有的医院网络设备都符合安全策略，从而大幅度提高网络的安全性，不受规模和复杂性的影响。通过积极抵御蠕虫、病毒、间谍软件和恶意软件的攻击，机构可将注意力放在主动防御上（而不是被动响应）。
- 通过著名制造商的广泛部署与集成来扩展现有思科网络及防病毒、安全性和管理软件的价值。
- 检测并控制试图连接网络的所有设备，不受其访问方法的影响（如路由器、交换机、无线、VPN和拨号等），从而提高医院永续性和可扩展性。
- 防止不符合策略和不可管理的终端设备影响网络可用性或用户生产率。
- 降低与识别和修复不符合策略的、不可管理的和受感染的系统相关的运行成本。

Cisco NAC提供三种关键的保护功能:

- 在验证授权点识别用户、用户设备及其在网络中的作用。
- 使用扫描和分析技术评估终端的安全状态，或使用轻型代理进行更深入的状态评估，以检查安全漏洞。
- 通过阻止、隔离和修复不符合策略的终端等方法在网络中执行安全策略。

NAC还提供以下实施优势:

- 可扩展性－CISCO NAC可直接部署，用于满足网络准入需求，同时设计并评估NAC框架，这是因为CISCO NAC组件可集成到更广泛的NAC框架架构中。
- 快速部署－CISCO NAC是现成的“紧缩型” 套装解决方案，针对防病毒、防间谍软件和MICROSOFT更新提供预装支持。
- 灵活性－CISCO NAC支持运行多个桌面操作系统的混合网络基础设施。

NAC方案组件:

- CISCO CLEAN ACCESS SERVER，评估设备并基于终端的策略符合情况授予访问权限。
- CISCO CLEAN ACCESS MANAGER，集中管理CISCO NAC解决方案，包括执行策略和修补服务。
- CISCO CLEAN ACCESS AGENT，可选的免费软件，提供更严格的终端策略符合评估，并同时简化可管理与不可管理环境中的修补流程。

3. 医院网络安全区域划分

现在的网络面临多种多样的安全威胁，医院需要建立纵深防御体系来防止因某个部分的侵入而导致整个系统的崩溃。只有基于网络系统之间逻辑关联性和物理位置、功能特性，划分清楚的安全层次和安全区域，在部署安全产品和策略时，才可以定义清楚地安全策略和部署模式。安全保障包括网络基础设施、业务网、办公网、本地交换网、信息安全基础设施等多个保护区域。这些区域是一个紧密联系的整体，相互间既有纵向的纵深关系，又有横向的协作关系，每个范围都有各自的安全目标和安全保障职责。积极防御、综合防范的方针为各个保护范围提供安全保障，有效地协调纵向和横向的关系，提高网络整体防御能力。

针对医院的网络系统，我们可以根据物理位置、功能区域、业务应用或者管理策略等等划分安全区域。不同的区域之间进行物理或逻辑隔离。物理隔离很简单，就是建立两套网络对应不同的应用或服务，最典型的就是医院业务网络和互联网访问网络的隔离。而对于内部各部门或应用来说，我们经常采用的是利用防火墙逻辑隔离的方法。

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医院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医院网络。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。

而针对医院内部各种业务应用的安全控制，可将防火墙模块（FWSM）安装在Cisco Catalyst 6500系列交换机的内部，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。Cisco Catalyst 6500 真正成为了那些需要各种智能化服务（例如防火墙接入、入侵检测、虚拟专用网（VPN））和多层LAN、WAN和MAN交换功能的客户的首选IP服务交换机。

FWSM可以支持最高30Gbps的吞吐量，因而可以提供无以伦比的性能，让医院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中最多可以添加四个FWSM，以满足用户不断发展的需求。

FWSM可以部署在医院园区的数据中心的网络拓扑中。今天的医院不仅仅需要周边安全，还需要连接业务伙伴和提供医院园区安全区域，医院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医院中设立安全域，提供一种灵活、经济、基于性能的解决方案。利用FWSM，用户可以为不同的VLAN制定相应的策略。

医院数据中心也需要用状态防火墙安全解决方案来保护数据，并以尽可能低的成本提供千兆位的性能。FWSM可以通过在防火墙中提供最佳的性能价格比，最大限度地提高资本投资效率，让医院客户可以放弃过去那些需要另购防火墙负载均衡设备的、价格昂贵的防火墙产品。而且由于FWSM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。

4. 医院网络边界安全

互联网对各种规模的医院来说都十分重要。它带来了业务发展的新机遇。通过VPN连接，它使得医院可与合作伙伴和远程员工保持联系。但它也是将威胁带入医院网络的渠道，这些威胁可能会对医院造成重大影响:

- 病毒－可感染系统，使其停运，从而导致运行中断和收入损失。
- 间谍软件和黑客－会导致公司数据丢失和因此引起法律问题。
- 垃圾邮件和泄密－需要繁琐的处理过程，降低员工生产率。
- 浏览与工作无关的网站－会导致员工生产率降低，并可能使公司承担法律责任。
- 受感染的VPN流量－使威胁因素进入网络，中断业务。

Cisco ASA 5500系列提供了一体化安全解决方案，提供了一个易于使用、且具有医院需要的安全功能的全面安全解决方案，结合了防火墙、入侵保护、Anti-X和VPN功能，您可对您的医院网络受到的保护充满信心。通过终止垃圾邮件、间谍软件和其他互联网威胁，员工生产率得到了提高。IT人员也从处理病毒和间谍软件消除以及系统清洁任务中解放出来。您可集中精力发展业务，而无需为最新病毒和威胁担忧。

Cisco ASA 5500系列为医院提供了全面的网关安全和VPN连接。凭借其集成的防火墙和Anti-X功能，Cisco ASA 5500系列能在威胁进入网络和影响业务运营前，就在网关处将它们拦截在网络之外。这些服务也可扩展到远程接入用户，提供一条威胁防御VPN连接。

最值得信赖、广为部署的防火墙技术—Cisco ASA 5500系列构建于Cisco PIX 安全设备系列的基础之上，在阻挡不受欢迎的来访流量的同时，允许合法业务流量进入。凭借其应用控制功能，该解决方案可限制对等即时消息和恶意流量的传输，因为它们可能会导致安全漏洞，进而威胁到网络。

市场领先的Anti-X功能—通过内容安全和控制安全服务模块（CSC-SSM）提供的强大的Anti-X功能，Cisco ASA 5500系列提供了全面保护所需的重要的网络周边安全性。

防间谍软件—阻止间谍软件通过互联网流量（HTTP和FTP）和电子邮件流量进入您的网络。通过在网关处阻拦间谍软件，使IT支持人员无需再进行昂贵的间谍软件清除过程，并提高员工生产率。

防垃圾邮件—有效地阻拦垃圾邮件，且误报率极低，有助于保持电子邮件效率，不影响与客户、供应商和合作伙伴的通信。

防病毒—屡获大奖的防病毒技术在您基础设施中最有效的地点——互联网网关处防御已知和未知攻击，保护您的内部网络资源。在周边清洁您的电子邮件和Web流量，即无需再进行耗费大量资源的恶意软件感染清除工作，有助于确保业务连续性。

防泄密— 确定针对泄密攻击的防盗窃保护，因此可防止员工无意间泄漏公司或个人信息，以导致经济损失。

针对Web接入、电子邮件(SMTP和POP3)以及FTP的实时保护。即使机构的电子邮件已进行了保护，但许多员工仍会通过公司PC或笔记本电脑访问自己的个人电子邮件，从而为互联网威胁提供了另一个入点。同样，员工可能直接下载受到感染的程序或文件。在互联网网关对所有Web流量进行实时保护，可减少这一常被忽略的安全易损点。

URL过滤—Web和URL过滤可用于控制员工对于互联网的使用，阻止他们访问不适当的或与业务无关的网站，从而提高员工生产率，并减少因员工访问了不应访问的Web内容而承担法律责任的机会。

电子邮件内容过滤—电子邮件过滤减少了公司因收到通过电子邮件传输的攻击信息而承担法律责任的机会。过滤也有助于符合法律法规，可帮助机构达到Graham Leach Bliley 和数据保护法案等的要求。

威胁防御VPN—Cisco ASA 5500系列为远程用户提供了威胁防御接入功能。该解决方案提供了对内部网络系统和服务的站点间访问和远程用户访问。此解决方案结合了对于SSL和IPSec VPN功能的支持，可实现最高灵活性。因为这一解决方案将防火墙和Anti-X服务与VPN服务相结合，可确保VPN流量不会为医院带来恶意软件或其他威胁。

方便的部署和管理—随此解决方案提供了思科自适应安全设备管理器（ASDM），它具有一个基于浏览器的、功能强大、易于使用的管理和监控界面。这一解决方案在单一应用中提供了对于所有服务的全面配置。此外，向导可指导用户完成配置的设置，实现迅速部署。

另外，在当前的网络应用中，P2P应用泛滥，网络攻击、垃圾邮件、病毒泛滥，网络速度慢，网络出口拥塞，防火墙过载，但缺乏监控手段，QoS 部署效果很差。因此医院网络的出口管理也是一个很重要的值得重视的问题。

对用户及应用的识别是实现服务分级控制及分析的基础，医院管理者需要了解网络应用情况：有多少应用、流量从哪来、流量到哪去、用户做什么、多长时间、多少带宽等等。而现实的情况是，只知道有多少用户上网，用掉的总带宽；但对第7层的用户使用分析缺乏。在Internet 出口需要一个设备，可以基于每个用户、每个应用控制流量和Session 数目。

思科服务控制引擎（SCE），可以同时处理200万个并发数据流、10万个在线用户(IP)、有高达3.6Gbps的数据吞吐量，4个PPC 分担负载，对每个包都完全处理而不是抽样，可编程控制包识别和处理策略。

通过思科服务控制引擎，可以对邮件进行分析，显示每24小时邮件发送排名，从而找到潜在垃圾邮件发送人，显示每24小时邮件发送服务器排名，从而找到潜在垃圾邮件发送服务器；可以查看网络出网方向Web 网站访问的情况，显示网络出网方向Web 网站访问点击率排名、院外Web网站访问下载量排名；可以清楚了解用户情况，查看总用户数、BT用户数、每小时用户会话数量排名（潜在代理或病毒主机）；可以进行BT 控制；可以查看每小时发生DoS攻击的IP地址和攻击次数，并对可疑用户进行跟踪。

通过部署服务控制引擎SCE，医院能够了解互联网链路的使用状况，并对互联网链路上的业务进行控制，引导医院内部用户正确地使用互联网。并且能够能够把SCE提供的流量报告，作为网络安全的分析和规划的依据。

5. 核心医疗业务服务器和重点医护终端的安全防护

对于医院网络来说，除了考虑网络本身的安全外，怎样保护敏感数据，防止敏感数据从各种途径传播出去。同时要保证只有授权用户,授权应用或授权的网络范围才可以访问数据。需要有详细的安全控制，以确保证医疗数据安全。

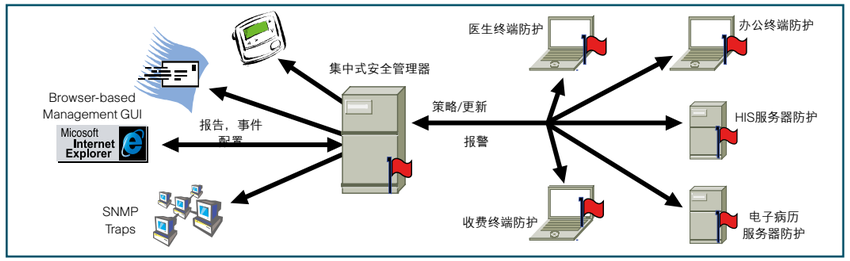
采用思科安全代理（Cisco Security Agent，CSA），可以保护重要的医疗应用服务器和客户端，实现零升级的结构。思科的思路是，不采用特征码，而是依靠行为规则，减少漏洞修补管理的费用，防止攻击。由于采用统一的安全代理，所以容易管理。

通过推出思科安全代理终端安全软件，思科可以为它的客户提供最全面的网络安全威胁防范产品保护敏感数据，以保护医院网络。其主要可实现的功能如下：

- 防止敏感数据从各种途径传播出去（USB盘、光驱、电子邮件、网络共享路径）。
- 防止文件被复制、被拷屏、被copy/paste泄漏出去。
- 授权用户才能访问。
- 授权应用才可以访问数据。
- 授权的网络范围才可以访问。
- 详细的audit：文件名、用户名、操作等。

新一代思科安全代理网络安全软件可以为HIS、PACS、LIS、移动医疗等核心医疗业务服务器和医生护士工作站等终端计算机提供威胁防范功能。思科安全代理与传统的终端安全解决方案的不同之处在于，它可以在恶意行为发生之前发现和阻止它们，进而消除潜在的已知和未知安全风险，防止其威胁到医院网络和应用的安全。因为思科安全

（图）思科安全代理CSA构成



代理采用的是分析行为而不是特征匹配的方法，因而这个解决方案能够以较低的运营成本提供强大的保护。

思科安全代理包括多个基于主机的代理，它们部署在关键任务型台式机和服务器上，向运行在CiscoWorks VPN/安全管理解决方案（VMS）上的管理中心进行报告。这些代理采用HTTP和安全套接字层（SSL）协议（128位SSL）建立管理接口和进行主机、管理中心之间的通信。所有配置都通过CiscoWorks VMS进行，而警报通过CiscoWorks安全监视器（SecMon）与来自于其他思科安全产品的警报集成到一起。

思科安全代理的管理中心可以通过CiscoWorks VMS平台集中地为所有的代理提供所有的管理功能。它的基于角色的、基于Web浏览器的、“从任何地方进行管理的”访问方式使管理人员可以方便地创建代理软件分发包、创建或者修改安全策略、监控警报或者生成报告。因为它预置了超过20多种完整的缺省策略，管理人员将能够方便地在整个医院中部署数以千计的代理。管理中心还可以让客户在“IDS模式”下部署代理。在这种模式下，活动会引发警报，但是不会被制止。

同时思科安全代理还具有控制光盘写入，USB端口等功能以防止有人恶意通过移动存储介质偷取医院的重要业务数据。

6. 医院网络安全管理

谈到安全管理，首先我们应该考虑的是网络的入侵检测或保护。互联网和电子商务的发展迫使各医院进入了一个开放、信任的通信时代。与此同时，这种开放性也带来了问题和弱点。因此必须采取相应的措施，防止医院宝贵数据受到入侵者、黑客和内部人员的损害。另一方面，当我们开始在交换式基础设施中部署越来越多的对内容敏感的服务的时候，必须提供前所未有的医院科研和核心医疗业务应用的可靠性。

Cisco IDS 4200系列设备检测器是专用型高性能网络安全“设备”，能够阻止网络上的非法恶意行为，例如黑客发动的攻击。Cisco IDS检测器能够实时分析流量，使用户能够快速对安全问题作出反应。

思科著名的思科防御研究小组（C-CRT）将许多高新检测技术结合在一起，包括状态样式识别、协议解析、启发式检测和异常检测，因而能有效消除多种已知和未知的计算机威胁。不仅如此，借助正在申请专利的Cisco签名微型引擎（SME）技术，还可以更加精细地定制检测器签名，精确调整检测器，减少“错误指示”的出现。

检测到非法行为后，检测器可以向管理控制台通报行为细节。另外，Cisco IDS主动响应系统还能控制路由器、防火墙和交换机等其它系统，为网络提供无与伦比的保护，及时中断非法操作。借助多种多样的管理解决方案，包括Web用户界面、命令行界面（CLI）或思科高度可扩展的CiscoWorks VPN/安全管理解决方案（VMS），这些设备的安装和管理非常容易。

对于当今市场上的多数入侵检测系统（IDS），必须将设备放置在交换端口分析器（SPAN）端口上才能监控网络流量。虽然SPAN端口可以提供对网络流量的访问，但它同时也存在着某些局限（例如，仅限于一定数量的SPAN对话和可信流量）。Catalyst 6000 IDS模块是专门为交换环境设计的，它直接将IDS功能集成到交换机中，由于可以直接从交换机背板上获取流量，因而可以在同一机架中同时实现交换和安全功能。

在黑客技术发展层面，以及越来越频繁爆发的网络危机来看，黑客们已熟悉了防火墙、 IDS等安全部件执行的传统访问控制策略。他们的攻击方式已不只是针对防火墙等产品的开放端口进行扫描，而是直指应用程序层面，寻找一切可以利用的漏洞。攻击手段越发复杂隐蔽和立体，如冲击波、震荡波等混合了蠕虫和黑客攻击等多重特性，对网络安全提出了新的挑战。

从另一个角度来看，医院在网络建设初期网络安全并没有很好地规划。随着网络建设的深入，安全产品不断增加，整体缺乏统一管理，相互间没有沟通交互，信息无法有效整合，是一些信息安全的孤岛。就象现在人们在关注和谈论的IT孤岛问题一样，各个应用系统之间缺乏有效联系，信息得不到整合，发挥不出其应有的价值。同样的问题放在网络安全上，这一效应就有可能放大成为风险，给企业IT系统的持续运转埋下隐患。

现在的防病毒软件有自己的管理系统，防火墙有自身管理系统，不同的系统有不同的网络管理软件，所以网络管理人员要保持对不同产品管理系统信息的检查。

其实这些来自不同安全产品的信息之间存在很大的相关性，如果分开独立地看待这些来自单一设备的信息，很有可能会忽略到一些重要的细节或关键因素，致使网络遭受重大打击。设想，当一个攻击发生时，防病毒、防火墙、IDS产品都发出了自身的报警信息，由于缺乏事件的关联性，一个事件会引起多个或大量的安全信息。这使网络管理人员无法进行及时处理，往往顾此失彼，手足无措，无法针对事件做出及时响应，迅速地给出一个良好、有效的解决办法。

不同安全产品的管理人员处理问题往往只针对自己产品本身，而没有统一调整整个网络的防御策略，这样往往会错过处理的最佳时机，而无法使企业网络在遭受病毒或攻击的时候，最大限度地减少所遭受的损失。

如果这种状况持续下去，网络安全管理员所看到的永远只是一个相对独立的安全信息，就像是那个盲人摸象的故事。看问题只是看到了一个角，而没有看到问题的全部，那些细节和隐藏在外表下的真相可能恰恰被忽略，而它们往往是问题的关键所在。像电信运营商这样拥有庞大的全国性网络、网络中安全产品数量众 多的大型企业，这种问题尤为突出。

我们传统的手段都是通过网络设备/安全设备发送Syslog到服务器上，作安全的事后审计。一个大型的网络，包含若干的网络产品，这些网络设备随时随地都在发送SysLog信息，每天产生的Log信息达到数万之多，任何一个网络管理员很难通过Syslog来准确定位网络发生的安全故障；即使有丰富知识的网络管理员，能通过Syslog分析得到有用的网络信息，但是速度也是很慢的。

思科安全监控、分析和响应系统（思科安全MARS）是一款基于设备的全功能解决方案，可提供针对医院现有安全部署的、前所未有的了解和控制能力。思科安全MARS是思科安全管理生命周期的一个关键组件，可帮助医院进行安全识别、管理和抵御安全威胁。它可充分利用医院现有的网络和安全投资，来识别、隔离被攻击的组件和建议对其精确删除的方式。它也有助于保持医院内部策略符合性，可作为整体法规符合性解决方案工具中一个不可缺少的部件。

医院安全和网络管理员所面临的问题有:

- 安全和网络信息过载
- 性能不佳的攻击和故障识别、优先级划分和响应
- 更高攻击先进程度、速度和修复成本
- 满足法规符合性和审查要求
- 较少的安全人员和预算

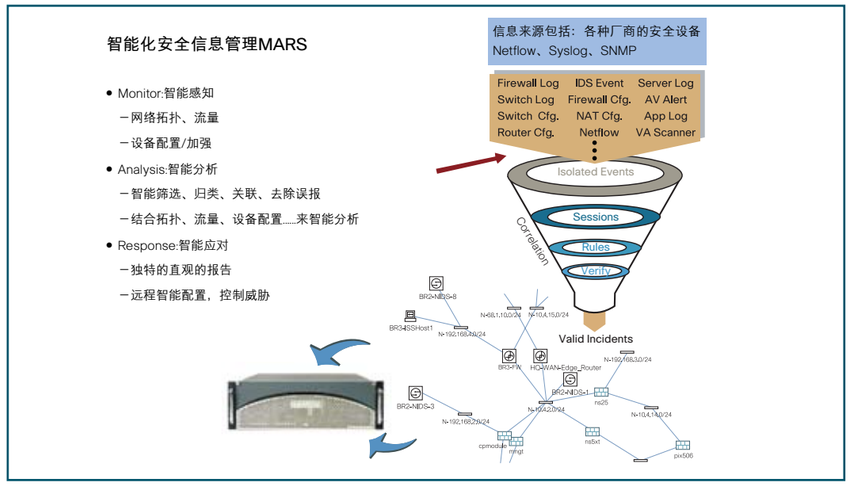
思科安全MARS可通过以下功能满足其需要:

- 集成网络智能，进行网络异常事件和安全事件的先进关联
- 察看校正后的事件并自动执行调查
- 通过全面充分利用网络和安全基础设施来防御攻击
- 监控系统、网络和安全运行来帮助医院达到法规符合性
- 以最低TCO提供一个易于部署和使用的、可扩展的设备
- 将网络安全设备大量的告警信息进行综合整理归纳使其具有可读性

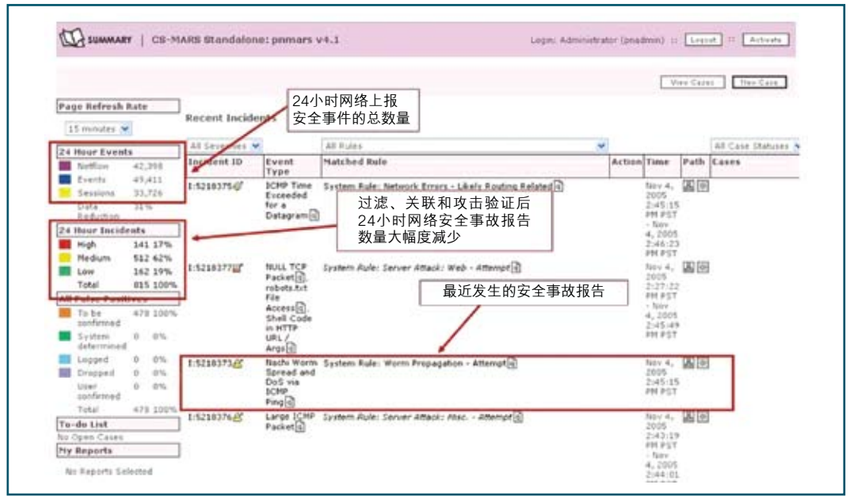
思科安全MARS可将原始网络和安全数据转化为可操作的智能特性，以提交正确有效的安全事件并保持法规符合性。这一易于使用的威胁防御设备系列可利用已部署在您的基础设施中的网络和安全设备，使操作员可集中、检测、防御和报告重要威胁。

思科安全MARS了解路由器、交换机和防火墙的拓扑和设备配置，以及网络流量配置，实现了网络智能。通过该系统的集成网络发现功能，可构建一个包括设备配置和当前安全策略的拓扑图，使思科安全MARS能对您网络中的分组流建模。因为此设备不在内部运行，极少使用现有软件代理，所以对网络或系统性能的影响极小。

（图）智能化安全信息管理MARS



（图）先知先觉，主动防御：总体报告和最新严重安全网络事件



这一设备集中汇总了来自各种常用网络设备（如路由器和交换机）、安全设备和应用（如防火墙、入侵检测、漏洞扫描器和防病毒软件）、主机（如Windows、Solaris和Linux系统日志）、应用（如数据库、Web服务器和验证服务器）以及网络流量（如Cisco NetFlow）的日志和事件。

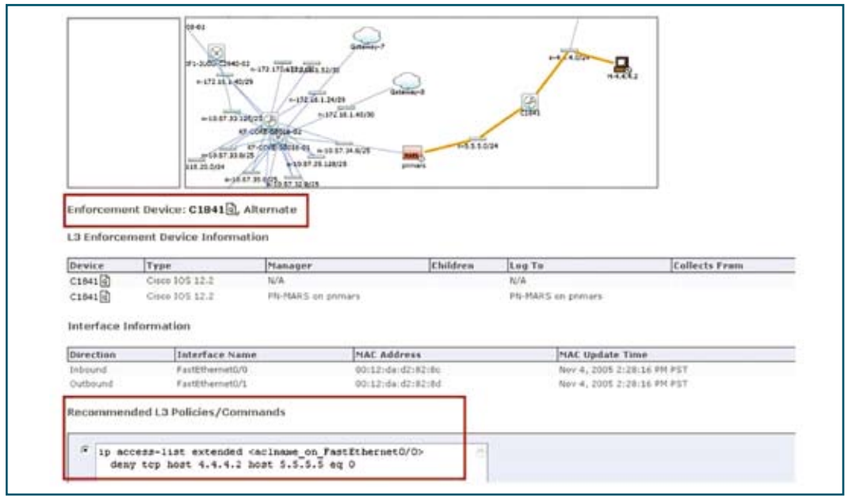
ContextCorrelation™在接收到事件和数据时，可针对网络拓扑、所发现的设备配置、相同的源和目的地应用（跨NAT边界）和类似的攻击类型，来对信息进行标准化。相似的事件会进行实时分组，随后对其运用由系统和用户定义的关联规则，来识别事故。系统配备了全面的预定义规则，Protego会经常更新这些规则，它们能识别大多数混合攻击、零日攻击和蠕虫。一个图形化规则定义框架简化了用户为任何应用创建定制规则的过程。ContextCorrelation大大减少了原始事件数据、实现了响应优先级划分并可最大限度地发挥所部署的措施的作用。

高性能汇总和整合。思科安全MARS解决方案可获取数千个原始事件，高效地对事件分类，实现前所未有的数据减少，并压缩这些信息以进行归档。管理大量安全事件需要一个安全、稳定的集中记录平台。思科安全MARS设备可安全地优化，接收极其大量的事件流量——每秒超过10000个事件或每秒超过30万个NetFlow事件。通过即将荣获专利的Protego内部处理逻辑和采用内嵌Oracle，这一切成为可能。所有数据库功能和调整都对用户透明。板载存储并可将历史数据档案持续压缩到NFS备用存储设备的功能，使思科安全MARS成为一个强大的安全日志/事件汇总解决方案。

7. 思科网络安全解决方案优势

未来的的计算机网络不仅仅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，做到既保护网络应用的同时，又保护了网络自身。而这正是思科所倡导的新一代的“自防御网络”计划。思科自防御网络计划是一种全新的多阶段安全计划，大大提高了网络发现、预防和对抗安全威胁的能力。适应未来信息系统发展的要求。思科为采用传统和新兴技术的综合应用环境提供了一个具高度永续性、响应能力和可扩展性的解决方案。

（图）攻击路径快感知并直接修复



网络威胁防御不是单独的设备添加，而是一个系统。安全已经变成了网络的一部分，已经和网络密不可分，安全无处不在。思科的网络安全解决方案包含了威胁防御、安全通信、安全的网络服务以及全方位的安全管理。涉及到网络安全的方方面面，融合了有线及无线网络，提供统一的安全策略。提供了业界最完整的安全解决方案，为整个医院业务应用的稳定运行保驾护航。

思科不仅仅可提供安全的解决方案或设备，同时可提供专业的安全服务，对整个系统进行安全评估，提出解决方案。并可针对医院业务应用需求提出网络安全设计策略。

3.3 思科医疗级网络安全保障解决方案设备参考

- 终端安全接入管理（根据终端数选择不同的配置，Manager可冗余配置）
  - －NACMGR-3-K9（Manager）+ NAC3310-250-K9（Server）
    终端数<250
  - －NACMGR-3-K9（Manager）+NAC3310-500-K9（Server）
    终端数200-500
  - －NACMGR-20-K9（Manager）+ NAC3350-1500-K9（Server）
    终端数500-1500
- 网络出口安全防御
  - －ASA5520-AIP40-K8/ ASA5540-AIP40-K8 一体化安全防御设备
- 内网安全区域的划分与高性能的安全隔离
  - －WS-SVC-FWM-1-K9 Catalyst 6500交换机上用的防火墙模块
- 网络出口流量管理
  - －SCE1010-2XGBE-MM
  - －SCE2020-4XGBE-MM
- 主机入侵防护
  - －CSA-START-6.0-K9 基本包
  - －CSA-B10-SRVR-K9 服务器license,可根据实际情况选择数量
  - －CSA-B25-DTOP-K9 桌面终端license，可根据实际情况选择数量
- 网络入侵检测及管理响应
  - － IPS-4240-K9/IPS-4255-K9/ IPS-4260-K9 独立的IPS
  - －WS-SVC-IDS2-BUN-K9 Catalyst 6500交换机上的入侵检测模块
- 网络安全管理
  - －CS-MARS-25-K9
  - －CS-MARS-55-K9

详细信息欢迎垂询思科区域医疗行业客户经理和医疗行业客户技术支持系统工程师，或参考思科网站：

- English：www.cisco.com
- 中文：www.cisco.com.cn

3.4 思科医疗级网络安全保障解决方案客户成功案例举例

北京大学人民医院

2003年，北京大学人民医院启动新一轮医院信息化建设，开始全面建设门诊信息系统、多分院集成的信息系统、门诊/住院医生工作站、PACS、与门诊/病房连网的检验信息系统等系统。而原有网络设备从性能，到可靠性都不能满足需要。同年，人民医院选择与思科公司合作，改造了人民医院的网络系统。

在制定解决方案时，北京大学人民医院重点考虑了当前系统管理的几个突出问题，如：网络的可靠性、安全性、瓶颈分析、网络优化、Internet安全、历史数据备份、灾难恢复、数据迁移、海量数据存储及存储安全、服务器的操作系统管理、数据库管理、中间件管理、数据库集群、中间件的集群与负载均衡、系统安全、客户机管理优化、网络防病毒及入侵检测等。

人民医院核心层采用两台思科公司的核心交换机Catalyst 6509，配置最新型的720G交换引擎，这主要是考虑医院未来几年信息系统发展的需要和设备的性能价格比，另外一个重要的原则是Catalyst 6509已经支持IPv6。

医院汇聚层采用两台Catalyst3550-24-SMI交换机，支持三层交换。通过光纤双链路上连到两台核心交换机Catalyst 6509，构成冗余主干。

人民医院充分利用Cisco Catalyst系列交换机强大的虚网管理功能，将网络划分成“安全、半安全及不安全”的子网，服务器子网必须绝对保证安全，严格控制其它机器连入权限和方式（数据库连接方式不传病毒）。

HIS使用的机器统一安装了病毒防火墙，除了统一安装的应用程序外，不允许用户安装任何其他应用程序。但由于允许这些极其使用文字处理程序和上网，不能保证绝对干净，但是一般不会造成大规模病毒流行并瘫痪。科研和办公的机器由于很难统一管理，主要采取隔离的方法。

人民医院在内网和外网之间采用了思科的ASA自适应安全设备进行隔离和安全通信，使内外网之间的信息可以安全地沟通，方便了业务的实现。

人民医院网络系统升级改造工程完成后，实际使用效果十分理想，为医院信息系统提供了稳定、可靠和安全的网络环境，并为未来建设数字化医院奠定了良好的基础。

哈尔滨医科大学附属第一医院

哈尔滨医科大学附属第一医院是一所集医疗、教学、科研为一体的大型综合性医院，全省最大的医疗中心，年门诊量超过100万人次，年急量7万人次，年出院病人量5万人次，年手术量4.2万例次，学院还承担着省内高干保健及外宾的诊疗任务，第一临床医学院是国家优秀示范临床教学基地，是全国高等临床医学教育中心培训分中心、全国高等临床医学教育中心远程教育培训学院第一分院，是全省两个专业技术人员继续教育基地之一。承担着研究生、七年制和五年制的临床教学任务，年在院学生2000余人，年接收进修医师350余人。

哈尔滨医科大学附属第一医院新建门诊大楼网络核心主干之间采用10GE互联，保证了医疗级网络的核心应用的高可用性。原有Catalyst 6509增加万兆模块双连接到新门诊楼核心的两台Catalyst 7609，新门诊楼内的两台Catalyst 7609万兆互联，与原Catalyst 6509组成万兆环网构成核心链路。全楼各科室及相关单位均采用千兆以太网技术通过三层架构（接入－汇聚－核心）和二层结构（接入－核心）接入医院网络核心。

由于哈尔滨医科大学附属第一医院网络上丰富的核心医疗业务应用，因此不但对网络可靠性有很高要求，对网络安全性的要求也尤为迫切，新门诊楼的两台Catalyst 7609分别配置一个防火墙模块（FWM）、入侵检测模块（IDSM）、网络分析（NAM），对医疗网细分安全隔离区域并进行高性能的安全通信，同时采取了先进的网络安全管理措施，非常显著地提高了网络的可用性。