白皮书

思科网络准入控制
常见问题问答

NAC 概述

什么是网络准入控制（NAC）?

思科网络准入控制（NAC）是一项由思科发起、多家厂商参加的计划，其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害。借助NAC，客户可以只允许合法的、值得信任的端点设备（例如PC、服务器、PDA）接入网络，而不允许其它设备接入。在初始阶段，当端点设备进入网络时，NAC能够帮助思科路由器实施访问权限。此项决策可以根据端点设备的信息制定，例如设备的当前防病毒状况以及操作系统补丁等。网络将按照客户制定的策略实行相应的准入控制决策：允许、拒绝、隔离或限制。一开始，NAC将支持运行Microsoft® Windows NT、XP和2000操作系统的端点设备。

NAC 的重要性何在?

零天病毒和蠕虫侵入将继续干扰企业业务的正常运作，造成停机，业务中断和不断地打补丁。利用思科网络准入控制，企业能够减少病毒和蠕虫对企业运作的干扰，因为它能够防止易损主机接入正常网络。在主机接入正常网络之前，NAC能够检查它是否符合企业最新制定的防病毒和操作系统补丁策略。可疑主机或有问题的主机将被隔离或限制网络接入范围，直到它经过修补或采取了相应的安全措施为止，这样不但可以防止这些主机成为蠕虫和病毒攻击的目标，还可以防止这些主机成为传播病毒的源头。

为全面保护网络，思科设计的 NAC 能够检测主机用于与网络连接的所有接入方法，包括通过WAN链路、IPSec远程接入和拨号连接的广域网关部署，以及通过交换和无线基础设施实施的局域网络部署。

思科 NAC 的开发是思科与领先防病毒安全厂商协作的结果，包括 Network Associates、Symantec 和 Trend Micro，其目的是查找易损系统，然后实施有效的网络准入控制。

应该部署 NAC 的理由

思科网络准入控制是一种防止易损主机和不符合要求的主机影响企业弹性的独特方法，借助它，客户能够充分利用现有网络和防病毒（AV）基础设施。NAC 的主要优点包括：

- 控制范围大——它能够检测主机用于与网络连接的所有接入方法，包括园区网交换、无线接入、路由器 WAN 链路、IPSec 远程接入和拨号

接入；

- 多厂商解决方案 —— NAC 是一项由思科发起、多家防病毒厂商参加的项目，包括Network Associates、Symantec 和 Trend Micro；
- 现有技术和标准的扩展 —— NAC 扩展了现有通信协议和安全技术的用途，例如可扩展认证协议（EAP）、802.1X 和 RADIUS 服务；
- 利用网络和防病毒投资—— NAC 将网络基础设施中的现有投资与防病毒技术结合在一起，提供了准入控制设施。

NAC 能够给企业带来哪些好处?

思科网络准入控制适用于需要防止病毒和蠕虫影响网络安全的所有组织。NAC对所有企业都有益处，尤其是自身很难管理台式机和服务器安全的机构，包括承包商和商业合作伙伴。基于同样的理由，NAC对小机构也很有用。NAC 几乎适用于所有的行业，例如金融、医疗、政府、制造等。

NAC 是否有利于操作系统和应用补丁管理?

是的。虽然 NAC 并不是一项操作系统或应用补丁管理技术，但是，如果与 Cisco Security Agent 配合使用，NAC 可以找到并隔离不符合要求和没有补丁的系统，使它们无法进入网络的其它部分，达到保护的目的。

思科为什么要与领先的防病毒厂商合作?

客户要求思科与领先的防病毒厂商合作，开发一种综合解决方案，以防止病毒和蠕虫对系统造成影响。思科与防病毒厂商密切合作开发的网络准入控制解决方案能够充分利用各厂商在网络和防病毒技术上的现有投资。NAC 将防病毒补丁合法性检查与网络准入控制结合在一起。 Network Associates、Symantec 和 Trend Micro 等领先的防病毒厂商代表了防病毒客户的大多数。

在开发 NAC 的过程中，思科与领先的防病毒厂商之间是什么关系?

在与领先的安全软件公司（Network Associates、Symantec 和 Trend Micro）合作的过程中，思科确立了 NAC 的体系结构、规范和共同营销规则。 思科向这些 NAC 合作者授予了端点软件技术许可证，以便将多个安全软件客户端的端点安装状况信息传送到制定和实施准入控制决策的思科网络。这个软件（Cisco Trust Agent）将与思科和 NAC 合作方的解决方案结合在一起，免费向客户提供。

思科还会与其它厂商合作吗?

目前，在执行NAC计划的过程中，为防止病毒和蠕虫破坏网络安全性，思科正与三家领先的防病毒厂商合作，他们是 Network Associates、Symantec 和 Trend Micro。得到客户运行实际经验的认可后，思科将

增加参与 NAC 的厂商的数量。

NAC 和思科安全策略

思科为什么要开发 NAC?

思科决心要解决当今客户面临的最重要的安全问题之一：各类病毒和蠕虫以各种方式影响企业的正常运作。蠕虫和病毒造成的损害说明，当前使用的运作和技术保护措施是不够的。借助 NAC 提供的新型综合解决方案，客户不但能实施主机补丁策略，还能限制或禁止有问题的或易遭受攻击的系统访问安全环境。借助端点安装状态信息，以及网络接入策略的实施，思科 NAC 能够帮助客户大大提高其计算基础设施的安全性。

什么是思科的自防御网络计划?

思科自防御网络计划是一种全新的多阶段安全计划，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。

NAC 与思科的自防御网络计划之间是什么关系?

思科网络准入控制是思科自防御网络计划中的一项，也是未来发展阶段的基础组件之一。

NAC 与思科 SAFE 蓝图之间是什么关系?

思科 SAFE 蓝图可作为正在考虑网络安全需求的网络设计师的指南。SAFE 针对网络安全设计采用了深入防御方法，它关注的是可以预测的威胁以及消除这些威胁的方法。由于采用了分层的安全方法，如果只有一个安全系统出现故障，将不会影响到整个网络的运作。

思科网络准入控制是一种新的安全解决方案，可用于消除病毒和蠕虫威胁。思科 SAFE 蓝图经过适当升级后，可以使用这种新型安全解决方案。

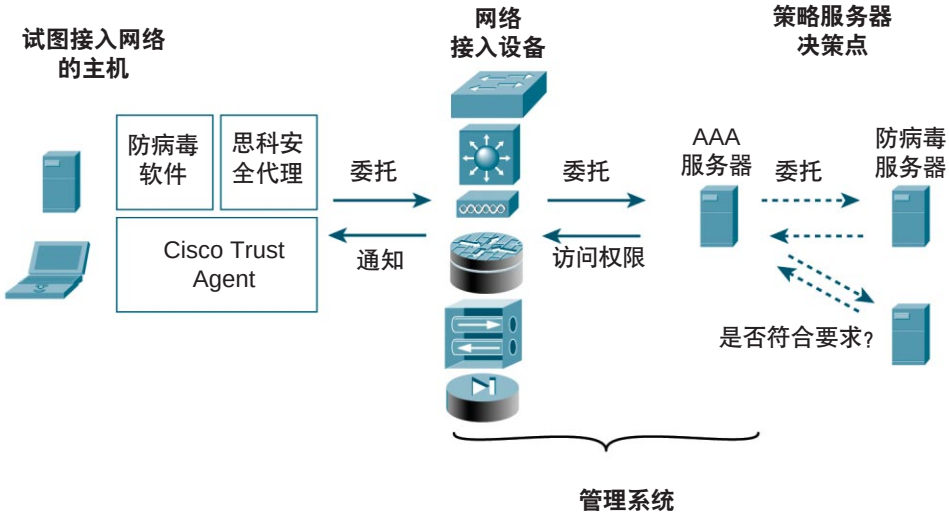
NAC 技术细节

NAC 系统的主要功能组件有哪些?

如下图所示，NAC 系统共包括四个组件：

[图形应该说明 CTA 与 AV SW 的分离]

图 1： NAC 系统的四个组件



- 端点安全软件（AV- 防病毒，Cisco Security Agent- 思科安全代理）与 Cisco Trust Agent ——思科信任代理从多个安全软件客户端收集安全状态信息，例如防病毒客户机软件，然后将这些信息传送到相连的思科网络，在那里实施准入控制决策。应用和操作系统状态信息，例如防病毒软件和操作系统补丁等级或信任关系，都可以用于制定相应的网络接入决策。思科和 NAC 合作商将把 Cisco Trust Agent 与自己的安全软件客户端集成在一起。

- 网络接入设备 ——实施准入控制的网络设备包括路由器、交换机、无线接入点和安全设备。这些设备接受主机委托，然后将信息传送到策略服务器，在那里实施网络准入控制决策。网络将按照客户制定的策略实施相应的准入控制决策：允许、拒绝、隔离或限制。

- 策略服务器——策略服务器负责评估来自网络设备的端点安全信息，并决定应该使用哪种接入策略。Cisco Secure ACS 服务器是一种认证、授权和审计 RADIUS 服务器，它构成了策略服务器系统的基础。它可以与 NAC 合作商的应用服务器配合使用，提供更强的委托审核功能，例如防病毒策略服务器。

- 管理服务器——思科管理解决方案将提供相应的思科NAC组件，以及监控和报告操作工具。CiscoWorks VPN/安全管理解决方案（CiscoWorks VMS）和CiscoWorks安全信息管理器解决方案（CiscoWorks SIMS）形成了此功能的基础。思科的 NAC 合作商将为其端点安全软件提供管理解决方案。

NAC的第一个版本通过了两项最严格的兼容性测试：防病毒软件状况和操作系统信息。它不但包括防病毒厂商的软件版本、机器等级和签名文件等级，还包括操作系统类型、补丁和热修复。以后还将继续扩大安全保护范围以及工作地点应用检查的范围。

什么是 Cisco Trust Agent?

Cisco Trust Agent 负责收集多个安全软件客户端的安全状态信息，例如 Anti-Virus 和 Cisco Security Agent 软件客户端，然后将信息传送到思科网络，在那里实施准入控制决策。Cisco Trust Agent 共有三个主要功能：

- 网络通信——响应对应用和操作系统信息的网络请求，例如防病毒和操作系统补丁细节，包括在第 2 层和第 3 层支持通信协议。
- 安全模型——对请求主机委托的应用或设备进行认证，并对传送的信息进行加密。
- 应用经纪人 ——通过应用编程接口（API）使多数应用能够响应状态和委托请求。

思科已经向 NAC 合作商授予了 Cisco Trust Agent 许可证，以便 Cisco Trust Agent 能够与合作商的安全软件客户端产品集成在一起。另外，思科还将 Cisco Trust Agent 与其安全客户机软件 Cisco Security Agent 集成在一起。思科与其 NAC 合作商都计划免费向客户提供 Cisco Trust Agent。

网络设备怎样与主机通信?

网络设备从主机请求应用和操作系统委托，互相传递请求与响应信息。可扩展认证协议（EAP）用于为认证打包并传送主机委托。所使用的主要传输协议共有两种：在第 3 层上使用 IP 的网关通信，以及使用 802.1X 的第一跳第 2 层通信。当网络设备离主机有任意跳，网络设备认为主机发出的都属于 IP 包时，可以用前面的一种方法部署，包括路由器、防火墙甚至远程接入通信。第二种方法通常由交换机在局域网内使用，也适用于带接入点的无线连接。

是否可以保证让主机运行兼容的防病毒软件?

可以。NAC 的第一个版本与领先防病毒厂商（Network Associates、Symantec 和 Trend Micro）的防病毒软件是连接在一起的。它不但能保证 AV 软件正常运行，还能保证软件、机器和样式文件版本符合客户策略的要求。这些信息将由 Cisco Trust Agent 汇总，然后传送到网络。对于未运行防病毒软件，或者没有适当版本的主机，按照预定策略，可以限制它对网络的接入范围，也可以其拒绝接入网络。此功能的第一个版本需要 Windows 平台的支持，包括 NT、XP 和 2000。

是否可以保证主机运行相应的 OS 补丁?

可以。Cisco Security Agent 是一种零天(day-zero)主机保护软件解决方案，它能够对操作系统版本、补丁和热修复信息进行评估，然后将这些信息传送给 Cisco Trust Agent。对于未运行适当补丁的主机，可以限制接入范围，或者禁止其接入。这个功能的第一个版本需要主要 Windows 平台的支持，包括 NT、XP 和 2000。

是否可以保证客户、承包商和合作伙伴的系统符合我制定的策略?

可以。思科网络准入控制可用于检查试图接入网络的每个系统，而不只是由 IT 管理的系统。无论是被管理的主机还是未被管理的主机，包括承包商和合作伙伴系统，都可以接受检查，看它是否符合防病毒策略和操作系统策略。如果接受检查的主机上没有安装 Cisco Trust Agent，将实施默认接入策略。对于未运行适当补丁的主机，可以限制接入范围，或者禁止其接入网络。

思科网络准入控制还支持不同厂商的防病毒软件。例如，如果某员工使用的是带 Cisco Trust Agent 的 Network Associates AV 解决方案，承包商使用的是带 Cisco Trust Agent 的 Symantec AV，这时，可以在同一个网络中检查每份委托书的合法性，然后按照用户身份和端点安全状态实施不同的策略。

支持哪些主机平台?

NAC操作适用于所有主机平台，但是，根据主机类型的不同，可能会在主机上执行不同等级的详细评估。

- 响应性——主机运行 Cisco Trust Agent，先与网络通信，然后将安全软件、应用和操作系统信息从主机传送到网络进行评估。
- 非响应性 —— Cisco Trust Agent 不活跃（未安装或未运行），因而无法将应用和操作系统信息传送到网络的主机。

响应性设备的网络接入策略可以基于主机上可用的任何应用和操作系统检查，例如，防病毒和操作系统补丁等级。由于非响应性设备不传送这些信息，因此，它们的网络接入策略必须基于其它信息，例如 IP 地址。

每个NAC阶段都会增加用于评估响应性和非响应性设备的信息。对于前者，实现的方法是将更多的应用集成到 NAC 框架中，强化所作的检查。对于后者，实现的方法是提供其它远程评估检查，以确定设备类型和状态。

Cisco Trust Agent 最初将在 NT、XP 和 2000 等 Windows 平台上运行，以后将逐步扩展到其它操作系统上，发展成一种开放式框架，实现广泛的平台对接和支持。

如果主机不运行 Cisco Trust Agent，还能用 NAC 吗?

不运行 Cisco Trust Agent 的主机称为非响应性设备，因为它们不能响应对应用和操作系统的网络请求。

除响应性设备外，还可以为非响应性设备制定网络接入策略。在NAC的第一个版本中，非响应性设备可以按照 IP 地址等网络信息执行接入策略。在 NAC 的未来版本中，为深化策略选择条件，还将增加网络指纹和资产目录跟踪系统。

还能用什么其它方法处理不兼容主机，怎样才能使它们兼容?

NAC的主要目标是使管理员能够监控主机的接入资格，然后作出决定，允许或拒绝正常网络接入不兼容主机。多数情况下，限制接入的方法是只让主机与一部分网络通信，或者只提供与公用网段的连接。隔离系统的更高目标是：提供一个安全的环境，对不兼容系统进行改造，使它们成为兼容主机，方法是补充防病毒样式文件，或者使用操作系统热修复。

在NAC的第一个版本中，由路由器提供网络准入控制，访问控制表（ACL）可以用于路由器，以限制不兼容系统的接入。客户可以将ACL配置成专用系统，以限制不兼容主机与网络中其它系统的通信，例如，只允许与防病毒服务器通信，下载新的样式文件。

在后续阶段，当用交换机和无线设备支持 NAC 时，可以只让不兼容主机接入只驻留有修复服务器的 VLAN 网段。

是否总是拒绝不兼容主机接入?

不是，这只是管理策略之一。不兼容主机的处理取决于公司制定的策略。被发现的不兼容主机可能可以接入普通网络，也可能只能接入公共网段或修复网段，还可能直接被拒绝接入。许多情况下，不兼容设备的处理取决于它们所在的位置。例如，可以完全禁止不兼容实验室机器与生产网络通信，但对于不兼容用户台式机，则可以规定只让它们与修复服务器通信。

NAC 部署

哪些网络平台支持 NAC?

思科接入和中档路由器是支持NAC的初始平台，包括目前的1700-7200系列。在以后的版本中，将陆续扩展到思科交换机、无线接入点以及 VPN 集中器和防火墙等安全设备上。

NAC 第一阶段和后续阶段将支持的平台和设备型号清单将在以后给出。

怎样部署 NAC?

思科NAC可以全面控制主机用于接入网络的所有接入方法：园区网交换、无线接入、路由器WAN和LAN链路、IPSec 远程接入和拨号接入。虽然网络设备能够在计划的不同阶段支持 NAC，但我们还是列出了几种典型的部署情况，并在图中给予了说明。

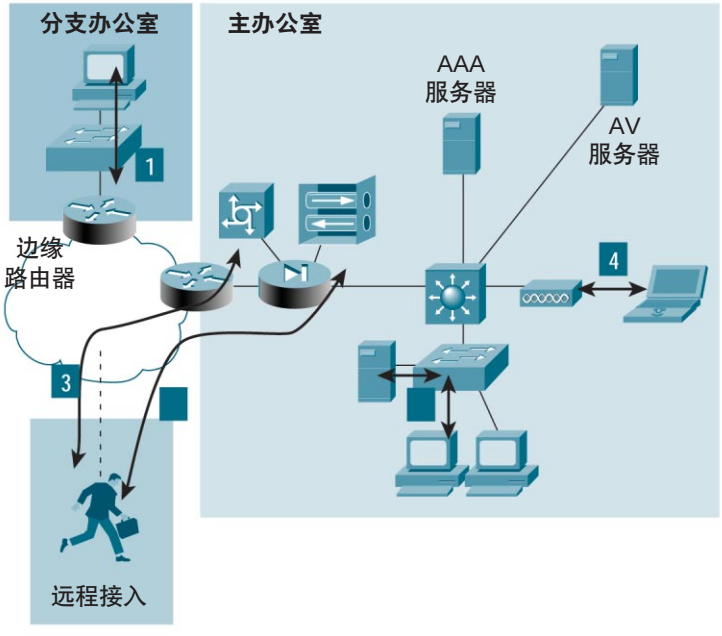
- 分支办公室（和 SOHO）兼容性 ——保证通过专用 WAN 或安全通道与公司中央资源连接的远程办公室或者小型和家庭办公室的主机是兼容的，包括在分支办公室出口路由器或主要办公室集中路由器处执行兼容性检查。
- 远程接入兼容性——远程员工和移动员工的台式机上安装了最新的防病毒软件和操作系统补丁之后才能通过 IPSec 及其它 VPN 连接访问公司资源。
- 拨号访问兼容性——与IPSec远程访问兼容性相似，可以保证使用传统拨号连接的主机符合公司制定的安全策略。
- 无线园区网保护——检查通过无线接入网络的主机，保证它们配备了适当的补丁。利用 802.1X 通信结合设备和用户认证执行此项审查。
- 园区网接入和数据中心保护 ——监控并保证，只有办公室里的台式机和服务器符合公司制定的防病毒和操作系统补丁策略，才能接入甚至最普通的局域网。这种方式能够将准入控制扩展到每个端口的第一跳第 2 层交换机，从而降低病毒和蠕虫在组织内传播的风险。

图 2：综合兼容性审查

部署情况

综合兼容性审查

1. 分支办公室兼容性
   在第 3 层路由器和防火墙上实施
2. 远程接入兼容性
   “你在那儿吗”的扩展
3. 拨号接入兼容性
4. 无线园区网保护
   利用 ACL/VLAN 隔离
   802.1x 的扩展
5. 园区网接入和数据中心保护



第一版 NAC 将首先部署在哪里?

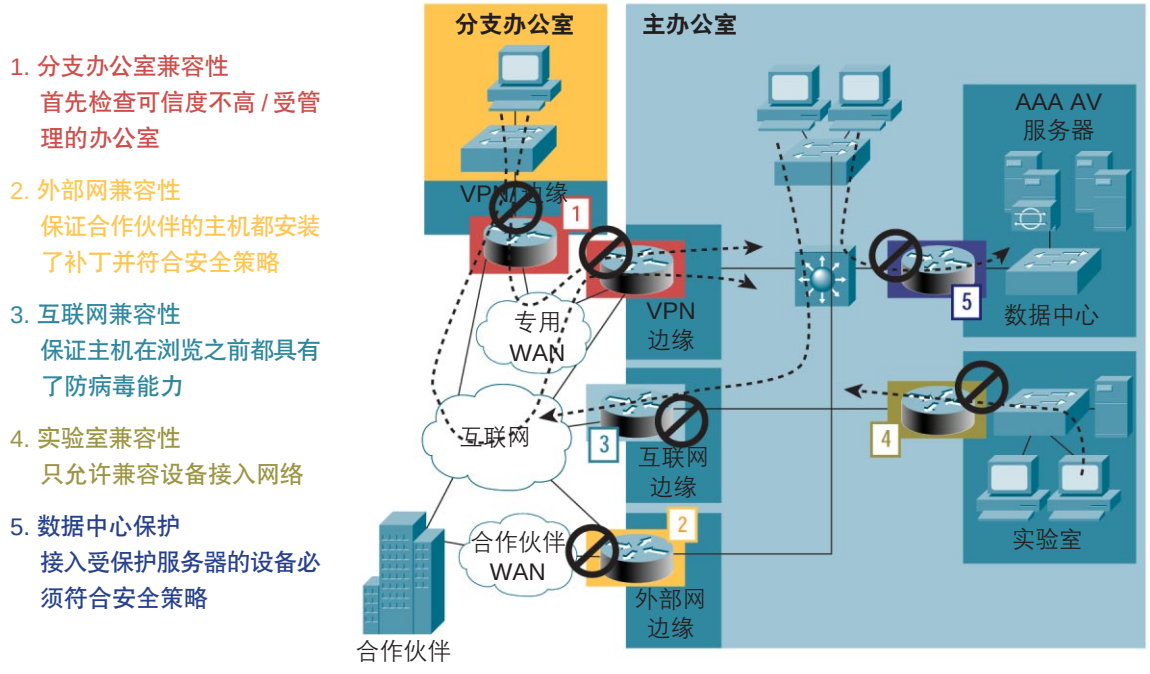
思科接入和中档路由器是支持NAC的初始平台。在许多实际部署中，都计划用路由器实现准入控制，其中多数部署已列在下面，并在图中给予了详细说明。

- 分支办公室（和 SOHO）兼容性 ——保证试图通过专用 WAN 或互联网安全通道与公司中央资源连接的远程办公室或者小型和家庭办公室符合安全要求，包括在分支办公室的出口路由器或主办公室集中路由器处执行兼容性检查。
- 外部网兼容性 ——保证合作机构管理的主机已配备了补丁，并符合公司策略。
- 互联网兼容性 ——在这种情况下，当被管理的主机试图与非管理区域或者互联网上的高风险区域通信时，将执行兼容性检查。
- 实验室兼容性 ——禁止实验室等非生产网段的主机与生产环境相连，除非它们安装了最新的安全补丁。
- 数据中心保护——在机构内建立安全岛，保护关键资源，只允许合法系统与之通信，从而降低安全风险。
- 远程接入保护 ——将路由器放置在远程接入汇聚集中器后面，保证主机符合防病毒和操作系统补丁策略（图中未说明）。

图 3：基于路由器的兼容性检查

第一阶段部署情况

基于路由器的兼容性检查



谁负责提供 NAC 的组件?

思科和 NAC 合作商负责提供准入控制解决方案的各种组件。

思科提供的以下组件将构成 NAC 的基础：

- 执行准入控制的网络设备包括路由器、交换机、无线接入点和安全设备。各种功能通过软件增强集成到新老平台中。
- Cisco Secure ACS 属于 AAA RADIUS 服务器，是用于确定接入权限的策略决策点。为支持 NAC，正在增强 ACS 功能。
- Cisco Trust Agent 属于主机代理，由思科开发，将通过多种方式分发：作为独立代理直接从思科或 NAC 合作商分发，与 Cisco Security Agent 一起分发，或者嵌入到 NAC 防病毒厂商的更新软件中。
- Cisco Security Agent 可以在主机上使用，同时为防止蠕虫和病毒提供零天保护，并为 NAC 提供操作系统补丁和热修复信息。
- CiscoWorks SIMS 是系统的监控和报告工具。
- CiscoWorks VMS 可用于在路由器上批量配置 NAC 设置。

Network Associates、Symantec 和 Trend Micro 将为主机和 AV 策略服务器提供系统的防病毒组件。

Network Associates 集成下面的部件：

.MaAfee VirusScan Enterprise

Sytemntec 将 Enterprise client security 和 AV 解决方案与 NAC 集成。

Trend Micro 集成下面的部件：

OfficeScan Corporate Edition

以后，还将继续增加 NAC 组件，例如用其它厂商工具评估主机状况和管理系统。

怎样获得 Cisco Trust Agent?

Cisco Trust Agent 可以嵌入到 NAC 合作商的防病毒软件中，可以与 Cisco Security Agent 一起嵌入，用户还可以直接从 Cisco Connection Online 或 NAC 合作商处获取。

怎样部署 NAC?

关于怎样部署NAC的详细信息将在临近初始版本推出的时候公布。一般情况下，部署的主要技术组件包括：

- 升级网络设备上的映像文件（例如新的 IOS 软件映像文件）
- 升级主机上的防病毒软件
- 主机上的 Cisco Trust Agent ——可以包含在防病毒软件升级过程中
- Cisco Secure ACS 服务器，用于执行兼容性评估和策略实施
- 用于配置、监控和报告 NAC 环境的管理工具

另外，还需要考虑以下操作问题：

- 确定管理权限模式，妥善管理系统，并相应调整管理组件
- 确定和实施网络准入控制策略
- 确定可扩展性和性能要求，保证系统可以应付高峰状况（尤其是 ACS 等策略决策基础设施）
- 确定和实施隔离和修复环境

最初部署 NAC 时，思科建议用户先检查策略符合程度，然后再实施相应的策略。在实施这个过程时，既要为报告而执行主机接入委托审查，又要保证正常的网络接入。决定实施安全检查的时机的依据是组织策略、准备程度以及威胁的严重程度。

网络设备怎样与主机通信?

网络设备从主机请求应用和操作系统委托，请求和响应在其间传输。可扩展认证协议（EAP）用于包装和传输主机委托，以便于认证。常用的两种主要传输协议包括：使用了 IP 的第 3 层网关通信以及使用了 802.1X 的第一跳第 2 层通信。当网络设备离主机有任意跳远，网络设备认为主机发出的所有数据都属于 IP 包时，使用第一种协议，包括路由器、防火墙设置远程接入通信。第二种协议适合在局域网内由交换机使用，或者用于建立带接入点的无线连接。

实施 NAC 时需要新的 AAA 服务器吗?

是的。Cisco Secure ACS 服务器正在为支持 NAC 而不断增强，它是必要的系统组件。ACS 将继续执行传统的 RADIUS 和 TACACS+ 服务，例如用户和设备认证和授权（AAA），借助这些新功能，ACS 将能够为用户、设备、操作系统和应用状态执行 AAA。另外，思科还将与 RADIUS 领域的业界领先厂商合作支持 NAC。

怎样执行准入控制?

首先由网络接入设备发出消息，从主机请求委托书。然后，AAA 服务器 Cisco Trust Agent（CTA）与主机上的 Cisco Trust Agent（CTA）建立安全的 EAP 对话。此时，CTA 对 AAA 服务器执行检查。委托书可以通过主机应用、CTA 或网络设备传递，由思科 ACS 接收后进行认证和授权。某些情况下，ACS 可以作为防病毒策略服务器的代理，直接将防病毒软件应用委托书传送到厂商的 AV 服务器接收检查。

委托书通过审查后，ACS 将为网络设备选择相应的实施策略。例如，ACS 可以向路由器发送准入控制表，对此主机实施特殊策略。

对于非响应性设备，可以对主动运行 CTA（网络或 ACS）的设备实施默认策略。在以后的各阶段，还将通过扫描或其它机制对主机系统执行进一步检查，以便收集其他端点安全信息。

网络设备怎样与 AAA 基础设施通信?

RADIUS 是网络设备与 Cisco Secure ACS 之间使用的协议。

AAA 服务器和 NAC 合作商的防病毒服务器怎样参与 NAC?

Cisco Secure ACS AAA 服务器的责任包括：检查主机的委托书，看它是否具备了应用和操作系统补丁；确定适用的网络接入策略；产生相应的审计记录，对系统进行监控。某些情况下，ACS 可以作为应用委托认证的代理，将相关信息传送到独立的应用策略服务器。例如，ACS可以将防病毒软件委托传送到AV策略服务器进行评估。在这种情况下，应用策略服务器首先对信息进行评估，然后向ACS传递一块令牌，确定兼容水平：完全兼容、部分兼容或不兼容。这种代理通信与AAA服务器检查当今用户常用的一次性令牌传送的过程非常相似。接下来，ACS 将把这块令牌与相应的策略对应起来，用适当的准入控制设置更新网络设备。

NAC 解决方案生态系统将怎样扩展?

思科正与NAC防病毒合作商通力合作，以便在第一版中提供相应的解决方案，执行AV和操作系统兼容性检查。在后续版本中，思科希望扩大 NAC 合作厂商的范围，融入其它安全软件和操作系统厂商。另外，思科还将发放许可证，公布和开放NAC接口和协议，加快Cisco Trust Agent的部署和NAC的采用。思科希望，这种方式将能够满足对其它端点和设备的 NAC 要求，例如 PDA。

这些组件是否基于标准?

思科网络准入控制采用了基于标准的技术，例如 EAP、UDP 上的 EAP、802.1X 和 RADIUS。某些情况下，这些技术可能需要增加一些专用功能才能支持NAC解决方案。思科希望通过相应的标准组织促进增强功能的采用。

NAC 将于何时上市?

思科网络准入控制分多个阶段实施，第一阶段将于2004年中期开始。这个阶段将在思科接入和中档路由器中支持 NAC。在正常接入网络之前，这些路由器要求在 Windows NT、XP 和 2000 设备上安装防病毒和操作系统补丁。对于不符合要求的主机，路由器可以限制它的接入范围，也可以完全禁止它接入网络。第一阶段应实现的功能包括：

- 对 NAC 提供 IOS 接入和中档路由器支持（请参考下面用于说明使用案例的部署方法问答）
- 在 Windows NT、XP 和 2000 平台上执行防病毒和操作系统补丁检查
- 评估防病毒软件状况
  - o Network Associates、Symantec 和 Trend Micro AV 解决方案
  - o 检查厂商、软件版本和样式文件版本等字段
- 评估操作系统版本、补丁和热修复水平
- 对 IP 地址定义表进行过滤，实施或忽略 NAC 检查；对不响应审查查询的主机实施统一的策略
- 检查 Cisco Security Agent 是否存在以及存在状态

在以后各阶段，NAC功能将被扩展到多个思科产品平台上，包括交换机、接入点和安全设备。其它功能将包括：

- 增加支持NAC的网络设备种类，包括交换机、无线接入点和安全设施
- 提供其它操作系统支持，执行补丁检查
- 提供更丰富的应用和操作系统状态检查（在防补丁和基本 OS 补丁水平检查之上）
- 对非响应性设备实施指纹检查和资产目录评估，以区分策略应用（例如，对动态发现的打印机或 IP 电话实施不同于非响应性 Windows XP 主机的策略）。

NAC 第二阶段的主要目标是提供交换机和无线支持，将网络设备与主机之间的通信协议从第3层和IP扩展到第 2 层和 802.1X。

如何获得更详细的信息?

如果想详细了解思科网络准入控制，请访问以下站点：

- 提供 NAC 信息的思科 web 站点：www.cisco.com/go/selfdefend
- 或者与当地的思科销售代表联络

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) 6528999

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