



VPN 和安全产品

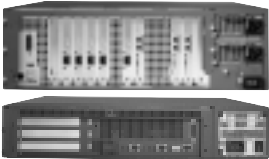
VPN 和安全产品一览

产品	特性	页数
Cisco PIX 安全设备	市场领先的、针对特定需求而设计的安全设备，可以提供范围广泛的集成化安全服务。 - 强大的状态化检测防火墙功能，带先进的应用和协议检测 - 高性能、可扩展的远程接入和站点间 VPN - 内嵌入侵防御，可以对网络攻击做出实时的反应 - 广泛支持多媒体和 VoIP 应用 - 荣获大奖的故障状态化恢复功能，可以提供企业级永续性	5-2
用于 Catalyst 6500 的防火墙模块	防火墙模块是一个面向 Catalyst 6500 系列交换机、高性能、集成的状态化防火墙解决方案，数据处理性能超过 5Gbps。它建立在经过验证的 PIX 技术的基础之上，可以为客户提供下列优势： - 投资保护 - 降低运营成本 - 易用性 - 统一运营 - 可扩展性 请参见第二章——局域网交换机中对 Catalyst 6500 系列交换机的介绍（2-24 页），了解更多相关信息。	2-24
思科安全代理	思科安全代理可以通过发现和防范恶意行为，防止桌面和服务器计算机系统受到安全威胁： - 汇聚并扩展多种终端安全功能 - 防御服务器和桌面上的已知和未知攻击，防御全部攻击类别，包括端口扫描、缓冲溢出、特洛伊木马、畸形分组、恶意 HTML 请求和电子邮件蠕虫 - 无需升级特征库，即可终止各种新增未知的攻击，并降低与部署升级相关的安全管理成本 - 可扩展到每台管理服务器 100,000 个代理 - 与 SDN/NAC 思科信任代理兼容。与 Cisco PIX、Cisco Secure IDS、Cisco VPN 安全设备和内置 Cisco Secure VPN “Are You There” (AYT) 集成管理	5-6
基于 Windows 的思科安全访问控制服务器 (ACS)	为思科智能信息网络提供全面的身份识别网络解决方案和安全用户体验。它是所有企业用户、管理员和网络基础设施资源间的集成和控制层。	5-7
思科安全访问控制服务器 (ACS) 解决方案引擎	一个高性能、高度可扩展的用户和管理访问控制解决方案，在交钥匙的安全增强解决方案中，可用作集中式 RADIUS 或 TACACS+ 服务器系统	5-9
思科安全用户注册工具 (URT)	确认用户在网络中的身份，创建用户注册策略捆绑，有助于支持移动性和跟踪： - 确保用户与他们获得授权的子网/虚拟局域网相关联 - 解决园区用户的移动性所带来的问题 - 可以在 Windows、Macintosh 和 Linux 客户端平台上支持基于 Web 的身份验证 - 通过基于 MAC 地址的安全选项，保护用户对 VLAN 的接入 - 所提供的选项让多个客户可以连接到一个集线器，从而接入某个基于一个交换机端口的虚拟局域网	5-10

产品	特性	页数
CiscoWorks VPN/安全管理解决方案	集成了各种用于配置、监控和诊断企业网络的常用设备管理工具，并且为管理虚拟专用网（VPN）、防火墙，以及基于网络和主机入侵检测系统（IDS）提供了功能强大的安全解决方案。作为面向企业的思科SAFE蓝图的组件，这个捆绑还提供了网络设备库存、变更审查和软件分发特性。CiscoWorks VMS划分为几个功能领域：防火墙管理、IDS管理、基于网络和服务、VPN路由管理、安全监控、VPN监控和运营管理。 参见第九章——Cisco IOS 软件和网络管理，了解更多关于 CiscoWorks VPN/安全管理解决方案的信息。	9-12
CiscoWorks 安全信息管理解决方案和 CiscoWorks 安全信息管理解决方案引擎	该解决方案可收集、分析并关联企业中的安全事件数据—让您可在发生安全事件时发现它们并作出响应。 • 对多供应商安全环境的事件监控 • 为操作员和高级管理员提供详细报告 • 提供的风险评估信息可使您了解企业中关键网络资产的总体易损性；为调查攻击提供分析工具 • 流量利用率报告和图形可使您了解流量模式的变化 参见第九章——Cisco IOS 软件和网络管理，了解更多关于 CiscoWorks VPN/安全管理解决方案的信息。	9-14
Cisco IOS 防火墙	• 与 IOS VPN 和高级路由技术紧密集成 • 通过为 TCP、UDP、SIP、Skinnny、H.323 等提供的、基于环境的访问控制（CBAC），实现了应用感知状态化分组检测 • 支持用户对 https、ftp 和 telnet 连接的验证 • 通过路由器专用域或使用外部 Websense 和 N2H2 服务器，进行 URL 过滤 • 内嵌入侵防御，可实时响应网络攻击，支持 100 种常用攻击特征 • 经由 TACACS+ 和 RADIUS，进行动态、网络到网络、逐个用户的验证和授权	5-11
思科安全路由器捆绑	带增强集成网络安全安全的 Cisco 800、1700、1800、2600、2800、3700、3800、7200 和 7301 安全路由器捆绑。请参阅各个产品所在页，了解更多信息（1-1）。	1-1
Cisco 800、1700、1800、2600、2800、3700、3800、7200 和 7301	广泛的模块化路由器平台，可以选择基于IOS的或由硬件实现的VPN、Cisco IOS Firewall、入侵防御、网络准入控制（NAC）和安全支持。	1-1

Cisco PIX 安全设备系列

世界领先的Cisco PIX® 安全设备系列在经济有效、便于部署的解决方案中，提供了企业级的集成网络安全服务，包括状态化检测防火墙、虚拟专用网（VPN）、入侵防御、多媒体和语音安全。Cisco PIX 安全设备的适用范围从面向小型办公机构的紧凑型、“即插即用”桌面防火墙到面向要求最严格的企业和服务供应商环境的运营商级千兆防火墙，为各种规模的网络环境提供强大的安全性、性能和可靠性。



适用场合

销售该产品

PIX 501

当客户需要以下这些特性时

- 小型办公机构 / 家庭办公机构桌面集成式安全设备
- 最高 60Mbps 防火墙吞吐量
- 高达 3Mbps 3DES 和 3.4Mbps AES-256 IPsec VPN 吞吐量¹
- 硬件 VPN 客户端（Easy VPN Remote）
- 最多可以为 10 个远程用户提供 VPN 集中器服务（Easy VPN Server）
- 集成 4 端口 10/100Mbps 交换机

PIX 506E

- 远程办公机构 / 分支机构桌面集成式安全设备
- 最高 100Mbps 防火墙吞吐量
- 高达 16Mbps 3DES 和 30Mbps AES-256 IPsec VPN 吞吐量¹
- 硬件 VPN 客户端（Easy VPN Remote）
- 最多可以为 25 个远程用户提供 VPN 集中器服务（Easy VPN Server）
- 最多 2 个 10BASE-T 以太网接口
- OSPF 动态路由支持

销售该产品

PIX 515E

当客户需要以下这些特性时

- 中小型企业 (SMB) 桌面集成式安全设备
- 最高 190Mbps 防火墙吞吐量¹
- 利用硬件加速 (某些型号自带, 在其他型号中为可选组件) 最高可以提供 130Mbps 3DES/AES-256 VPN 吞吐量¹
- 最多可以为 2000 个远程用户提供 VPN 集中器服务 (Easy VPN Server)
- 最多 6 个 10/100 FE 接口
- 虚拟局域网中继 (基于 802.1q 标签) 和 OSPF 动态路由支持
- 主 / 备用状态故障恢复支持

PIX 525

- 大型企业级集成式安全设备
- 最高 330 Mbps 防火墙吞吐量¹
- 利用硬件加速 (某些型号自带, 在其他型号中为可选组件) 最高可以提供 145 Mbps 3DES 和 135Mbps AES-256 VPN 吞吐量¹
- 最多可以为 2000 个远程用户提供 VPN 集中器服务 (Easy VPN Server)
- 千兆以太网支持, 最多 8 个 10/100 FE 或者 3 个千兆以太网接口
- 虚拟局域网中继 (基于 802.1q 标签) 和 OSPF 动态路由支持
- 主 / 备用状态故障恢复支持

PIX 535

- 运营高级大型企业和供应商防火墙设备
- 最高 1.7 Gbps 防火墙吞吐量¹
- 利用硬件加速 (某些型号自带, 在其他型号中为可选组件) 最高可以提供 425 Mbps 3DES/AES-256 VPN 吞吐量¹
- 最多可以为 2000 个远程用户提供 VPN 集中器服务 (Easy VPN Server)
- 千兆以太网支持, 最多 10 个 10/100 FE 或者 9 个千兆以太网接口
- 虚拟局域网中继 (基于 802.1q 标签) 和 OSPF 动态路由支持
- 冗余热插拔电源
- 主 / 备用状态故障恢复支持

1. 在分组大小为 1400 字节时

关键特性

- 安全性——针对特定用途制造的防火墙设备, 装有一个专用、强大的操作系统
- 性能——状态化检测防火墙能同时处理 500,000 个并发连接和高达 1.7Gbps 的吞吐量 (在 Cisco PIX 535 防火墙上, 分组大小为 1400 字节)
- 高可用性——屡获大奖的主 / 备用状态故障恢复模式可以提供大型企业级、经济有效的永续性
- 虚拟专用网 (VPN)——支持基于标准的 IPsec 和基于 L2TP/PPTP 的 VPN 服务
- 可选的 PIX VPN 加速卡 +——3DES/AES-256 VPN 吞吐量可以扩展到 495Mbps, 利用专用的协处理器来加快加密速度
- 免费的 Cisco VPN 客户端软件可以在多种平台之间提供安全连接, 这些平台包括 Windows、Mac OS X、Linux 和 Solaris
- 网络地址转换 (NAT) 和端口地址转换 (PAT)——隐藏内部的 IP 地址和拓展网址空间
- 拒绝服务 (DoS) 攻击防御——防止防火墙、内部服务器和客户端受到破坏性的黑客攻击
- OSPF 动态路由协议支持有助于提高系统的可靠性和性能
- 支持虚拟局域网 802.1q 标准, 可以简化在交换网络环境中的部署
- 为大量常用协议——H.323 v4、TAPI、JYAPI、RTSP、SIP、MGCP 和 SCCP 提供多媒体和 VoIP 支持
- 基于 Web 的 PIX 设备管理器 (PDM)——有助于简化配置、实时和历史报告、性能基线和安全事件信息
- 自动升级, 可以通过 SSH、SNMP、TFTP、HTTPS 和 Telnet 进行远程管理
- 支持范围从 2 个 10/100 以太网接口到 9 个千兆以太网接口

产品特性

特性	PIX501	PIX506E	PIX515E	PIX525	PIX535
处理器	133MHz	300MHz	433MHz	600MHz	1.0GHz
RAM	16MB	32MB	32 或 64MB	128 或 256MB	512MB 或 1GB
闪存	8MB	8MB	16MB	16MB	16MB
PCI 插槽	没有	没有	2	3	9
固定接口 (物理)	4个10/100交换机 端口 (内部), 1个 10Base-T 以太网 端口 (外部)	2个10BASE-T 以太网端口	2个10/100 快速以 以太网端口	2个10/100 快速以 以太网端口	没有
最大接口数量 (物理和虚拟 接口)	4个10/100交换机 端口 (内部), 1个 10Base-T 以太网 端口 (外部)	2个10BASE-T 以太网端口或2 个 VLAN	6个10/100 快速以 太网 (FE) 端口或 者8个虚拟局域网 端口	8个10/100 FE 端 口或者10个虚拟 局域网端口	10个10/100 FE或 GE 端口, 或者24 个虚拟局域网端口
VPN 加速器 卡+ (VAC+) 选项	没有	没有	有, 某些型号自带	有, 某些型号自带	有, 某些型号自带
故障恢复支持	没有	没有	有, 仅适用于 UR/ FO 型号	有, 仅适用于 UR/ FO 型号	有, 仅适用于 UR/ FO 型号
大小	桌面	桌面	1RU	2RU	3RU

部分产品编号和订购信息¹

Cisco PIX 捆绑

PIX-535-UR-BUN	PIX 535 无限制捆绑 (机箱、无限制软件、2个10/100 端口、VPN 加速卡+)
PIX-535-R-BUN	PIX 535 限制捆绑 (机箱、限制软件、2个10/100 端口)
PIX-535-FO-BUN	PIX 535 故障恢复捆绑 (机箱、故障恢复软件、2个10/100 端口、VPN 加速卡+)
PIX-525-UR-GE-BUN	PIX 525 无限制 GE 捆绑 (机箱、无限制软件、2个GE 端口、2个10/100 端口、VPN 加速卡+)
PIX-525-FO-GE-BUN	PIX 525 故障恢复 GE 捆绑 (机箱、故障恢复软件、2个GE 端口、2个10/100 端口、VPN 加速卡+)
PIX-525-UR-BUN	PIX 525 无限制捆绑 (机箱、无限制软件、2个10/100 端口、VPN 加速卡+)
PIX-525-R-BUN	PIX 525 限制捆绑 (机箱、限制软件、2个10/100 端口,)
PIX-525-FO-BUN	PIX 525 故障恢复捆绑 (机箱、故障恢复软件、2个10/100 端口、VPN 加速卡+)
PIX-515E-UR-FE-BUN	PIX 515E 无限制捆绑 (机箱、无限制软件、6个10/100 端口、VPN 加速卡+)
PIX-515E-FO-FE-BUN	PIX 515E 故障恢复捆绑 (机箱、故障恢复软件、6个10/100 端口、VPN 加速卡+)
PIX-515E-UR-BUN	PIX 515E 无限制捆绑 (机箱、无限制软件、2个10/100 端口、VPN 加速卡+)
PIX-515E-R-BUN	PIX 515E 限制捆绑 (机箱、限制软件、2个10/100 端口)
PIX-515E-FO-BUN	PIX 515E 故障恢复捆绑 (机箱、故障恢复软件、2个10/100 端口、VPN 加速卡+)
PIX-515E-R-DMZ-BUN	PIX 515E DMZ 捆绑 (机箱、限制软件、2个10/100 端口)
PIX-506E-BUN-K9	PIX 506E 3DES/AES 捆绑 (机箱、软件、3DES/AES 许可、2个10BASE-T 端口) 2
PIX-501-BUN-K9	PIX501 10 用户/3DES/AES 捆绑 (机箱、软件、10 用户/3DES/AES 许可、4 端口 10/100 交换机)
PIX-501-50-BUN-K9	PIX501 50 用户 /DES 捆绑 (机箱, SW, 50 用户 /DES 许可, 4 端口 10/100 交换机)
PIX-501-UL-BUN-K9	PIX501 无限制 /3DES/AES 捆绑 (机箱, 软件, 无限制 /3DES/AES 许可, 4 端口 10/100 交换机)

Cisco PIX 接口和卡

PIX-1GE-66	PIX 66MHz 千兆以太网接口卡 (多模光纤, SC 连接器)
PIX-4FE-66	PIX 66MHz 4 端口 10/100M 快速以太网接口卡, RJ45
PIX-1FE	PIX 单端口 10/100 快速以太网接口卡
PIX-VPN-ACCEL	PIX DES/3DES VPN 加速卡 (VAC)
PIX-VPN-PLUS	PIX DES/3DES/AES VPN 加速卡+ (VAC+)

PIX 附件

PIX-506E-PWR-AC

用于 PIX 506E 的冗余交流电源

PIX-515-PWR-DC

用于 PIX 515/515E 的冗余直流电源

1. 这里列出的仅仅是通过“详情垂询”的 URL 链接所能找到的所有产品的一小部分。有些产品设有一定的访问权限，或者无法通过分销渠道获得。经销商：要想获得最新的产品编号和订购信息，请访问分销产品查阅指南，网址是 <http://www.cisco.com/dprg>。（目前只限于部分国家）。

详情垂询

请访问 PIX 安全设备网站：<http://www.cisco.com/go/pix>

带集成网络安全的思科安全路由器捆绑

思科安全路由器捆绑适用于 Cisco 800、1700、1800、2600XM、2691、2800、3700、3800、7200 和 7301 路由器平台。它们包括入门安全捆绑、用于提高性能和扩大范围的增强安全捆绑，以及将安全和 IP 通信相结合的 V3PN 捆绑。

关键特性

- 订购思科路由器时只需单一产品编号，即能以低于独立订购每个组件的价格获得所有必要的安全组件
- 所有安全捆绑均预装了路由器和安全管理器，可在思科 TAC 和 ICSA 实验室建议的路由器安全配置的基础上，快速方便地进行部署
- 从 Cisco 800 系列开始提供捆绑 Cisco IOS，1711 和 1712 提供内嵌 VPN 加速
- Cisco 1700、2600XM、2691、3700、7200 和 7301 捆绑包括所选的路由器平台、一个 VPN 硬件卡、附加内存，以及运行 IPSec 3DES 或 AES 加密的 Cisco IOS
- Cisco 2600XM、2800、3700 和 3800 系列现拥有高级安全网络模块，可进行 URL 过滤和基于硬件的 IDS（入侵检测系统）
- 对于模块化平台，每个安全捆绑都有可选模块

适用场合

销售该产品

Cisco VPN 安全路由器捆绑

当客户需要以下这些特性时

- 防御从每个网关进入网络的蠕虫、病毒或威胁（NAC，防火墙，IPS）
- 在路由器上部署 VPN，需要获得更多未来的 VPN 选项
- 计划使用互联网进行远程业务通信（远程接入 VPN）
- 当从租用专线移植到 VPN 时
- 需加密来保护用户数据（如 HIPAA，Sarbanes-Oxley）
- 需集成语音和 VPN 服务（V3PN）
- 新型集成多业务路由器（Cisco 1800、2800 和 3800）有内嵌 VPN 加速，所以需相应的安全捆绑来实施 3DES 或 AES 加密功能

产品特性

特性	Cisco VPN 安全路由器捆绑
所有捆绑均包括的特性	采用 IPS 的网络准入控制 (NAC) 防火墙; GRE 和 IPSec; 高可用性/故障恢复; VPN QoS; 硬件中的 AES (不包括 C1700 捆绑)
IPPCP 压缩	软件: C800, C1700 捆绑 硬件: Cisco 1800 捆绑, C2600XM, C2691-VPN, Cisco 2800; 1500; C3725-VPN, C3745-VPN, Cisco 3800, 7200 和 7301 捆绑
最大隧道数	C800 - 10, C1700: 100; Cisco 1800: 800, C2600XM, C2691-VPN: 800; Cisco 2800: 1500; C3725-VPN, C3745-VPN: 2000; Cisco 3800: 2500; 7200/7301 捆绑: 5000
防火墙性能	C800 - 10Mbps, C1700: 20Mbps; Cisco 1800: 125 Mbps, C2600XM: 35Mbps; C2691-VPN: 197Mbps; Cisco 2800: 530Mbps; C3725-VPN, C3745-VPN: 197 Mbps; Cisco 3825: 855Mbps; Cisco 3845:1 Gbps, 7200/7301 捆绑: 1Gbps

详情垂询

更多信息请参见第一章：路由器。

思科安全代理

下一代思科安全代理网络安全软件可以为服务器和桌面计算系统（也被称为“终端”）提供威胁防御功能。思科安全代理可以在恶意行为发生之前发现并阻止它们，从而消除威胁到企业网络和应用的 风险，因此超越了传统的主机和桌面安全解决方案。思科安全代理可以通过在一个单一的代理设备中提供主机入侵防御、分布式防火墙、恶意移动代码防御、操作系统完整性保障和审查日志整合功能，集成和拓展多终端安全功能。

思科安全代理主要分析攻击行为，而不是依靠特征匹配，因而它的解决方案可以在提供强大的保护的同时降低运营成本。它提供了补丁来降低系统管理工作负载，使公司能获得厂商不断改进的“增强版”和服务包。升级的测试和实施能事先安排，不会出现不适当的变更干扰运营的现象。因更新较少，所以降低了拥有成本。

适用场合

销售该产品

思科安全代理

当客户需要以下这些特性时

- 思科安全代理可以通过一个单一的集成包提供主机入侵防御、分布式防火墙、恶意移动代码防御、操作系统强化、文件完整性和 / 或审查日志整合功能
- 防范已知和未知的攻击
- 保护服务器和 / 或台式机 / 笔记本电脑
- 一个可以通过扩展保护数千台服务器和台式机的解决方案，适用于大型企业部署
- 提供终端保护，使企业能安全地参与电子商务，并利用互联网经济

关键特性

- 可以为 Unix 和 Windows 服务器提供业界领先的保护
- 在单一代理中提供多种安全功能
- 开放、可扩展的架构让用户可以按照企业策略制定和实施安全措施
- “无需升级”，即可防御已知和未知攻击
- 可与思科网络安全产品集成
- 提供应用库存和使用跟踪、热修复和 Service Pack 状态检查，以及针对 Symantec 和 McAfee 防病毒代理的防病毒 DAT 版本检查
- 是用以保护电子商务的 SAFE 蓝图的一个关键组件

产品特性

特性	思科安全代理服务器版	思科安全代理台式机版	思科安全代理管理器版
平台	Windows 2000 Server 和 Advanced Server (最高 Service Pack 3) Windows NT v4.0 Server 和 Enterprise Server (Service Pack 5 或者更高版本) Solaris 8 SPARC 架构 (64 位内核)	Windows NT v4.0 Workstation (Service Pack 5 或者更高版本) Windows 2000 Professional (最高 Service Pack 3) Windows XP Professional (最高 Service Pack 1)	Windows 2000 Server 和 Advanced Server (最高 Service Pack 2)

部分产品编号和订购信息¹

思科安全代理选项

CSA-SRVR-K9=	思科安全代理服务器版 (Win 和 Sol), 1 个代理
CSA-B10-SRVR-K9	思科安全代理服务器版 (Win 和 Sol), 10 个代理捆绑
CSA-B25-SRVR-K9	思科安全代理服务器版 (Win 和 Sol), 25 个代理捆绑
CSA-B50-SRVR-K9	思科安全代理服务器版 (Win 和 Sol), 50 个代理捆绑
CSA-B100-SRVR-K9	思科安全代理服务器版 (Win 和 Sol), 100 个代理捆绑
CSA-B25-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 25 个代理捆绑
CSA-B100-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 100 个代理捆绑
CSA-B250-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 250 个代理捆绑
CSA-B500-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 500 个代理捆绑
CSA-B500-SRVR-K9	思科安全代理服务器版 (Win 和 Sol), 500 个代理捆绑
CSA-B1000-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 1000 个代理捆绑
CSA-B5000-DTOP-K9	思科安全代理台式机版 (Win 和 Sol), 5000 个代理捆绑
CSA-PROFILER-K9	思科安全代理配置器

注意

出口注意事项: 思科安全代理在出口时要受到一定的限制。请访问出口规定网站: <http://www.cisco.com/wwl/export/crypto/>, 了解相关规定。如有任何关于出口的问题, 请联络 export@cisco.com。

详情垂询

请访问思科安全代理网站: <http://www.cisco.com/go/csa>

基于 Windows 的思科安全访问控制服务器

思科安全访问控制服务器(ACS)是一个高度可扩展、高性能的访问控制服务器,可以充当一个集中式RADIUS或者TACACS+服务器。Cisco Secure ACS 通过在一个集中身份识别联网解决方案中将身份验证、用户或管理员接入及策略控制相结合,强化了接入安全性。它可以大幅度降低为用户和网络管理员提供对您的网络的接入权限所带来的管理负担。通过为所有用户帐户使用一个中央数据库,它可集中对所有用户权利的控制,并将其应用于网络中的数百或数千接入点,作为一种记帐服务。Cisco Secure ACS 可具体报告和监控网络用户行为,并保持对整个网络中每一接入连接和设备配置改变的记录,从而降低 IT 运营成本。Cisco Secure ACS 支持范围广泛的接入连接类型,包括有线和无线 LAN、拨号、宽带、内容、存储、IP 语音、防火墙和 VPN。

Cisco Secure ACS 是基于身份识别的思科联网服务 (IBNS) 架构和思科网络准入控制 (NAC) 的一个关键组件。

适用场合

销售该产品
基于 Windows 的思科安全接入
控制服务器（ACS）

当客户需要以下这些特性时

- 集中控制谁可以通过有线或者无线连接登陆网络
- 设置每个网络用户的权限
- 记录记帐信息，包括安全审查或者用户记帐
- 设置每个配置管理员的访问权限和控制指令
- 用于 Aironet rekey 的虚拟 VSA
- 安全的服务器身份验证和加密
- 通过动态端口分配简化防火墙接入和控制
- 统一的用户 AAA 服务

关键特性

- Cisco NAC 支持——使用您所配置的策略，它可评估由思科安全代理发送给它的证书，确定主机的状态，并发送与主机状态相对应的 AAA 客户端 ACL；记录策略评估的结果以供您的监控系统使用
- 支持思科开发的、新型、可公开接入的 IEEE 802.1X EAP 类型，以服务于不能实施强大密码策略的客户以及想部署一个 802.1X EAP 的客户；无需数字证书，支持各种用户和密码数据库类型、密码到期和更改，灵活、易部署、易管理
- 可下载的 IP 访问控制列表（ACL）——将每用户 ACL 支持扩展到所有支持此功能的第三层网络设备；可逐个用户或逐个组地应用定制 ACL
- 认证撤回列表（CRL）比较，可用于 EAP- 传输层安全（TLS）验证——增加了对使用 X.509 CRL 简况的认证撤回的支持；如果在 EAP-TLS 验证期间，用户所提交的证书在所查询的 CRL 中，则 Cisco Secure ACS 使该验证失效，拒绝该用户的接入要求
- 对 802.1X 机器验证构成补充的机器接入限制（MAR）——能使用 MAR 来控制根据 Windows 外部用户数据库而验证的 EAP-TLS 和 Microsoft 受保护可扩展验证协议（PEAP）用户的授权
- 作为一个新的共享配置组件的网络接入过滤（NAF）——可精确地对各设备分别应用网络接入限制和可下载 ACL，而以前只能对所有设备应用相同的接入限制或 ACL
- 可独立复制用户和组数据库

产品特性

特性	基于 Windows 的思科安全访问控制服务器（ACS）
硬件	• Pentium 处理器，550MHz 或更高 • 256MB RAM • 250MB 磁盘空间；如果您需要在同一台机器上运行您的数据库，则需要更多的磁盘空间 • 最低分辨率为 800 × 600，256 色

部分产品编号和订购信息¹

基于 Windows 的思科安全访问控制服务器 (ACS)	
CSACS-3.3-WIN-K9	Cisco Secure ACS 3.3 for Windows
CSACS-3.3-WINUP-K9	从 ACS 1.x、2.x 和 Cisco Secure ACS for Unix 2.x 版本升级到 CSACS 3.3 for Windows
CSACS-3.3-WINMR-K9	次要版本升级工具，用于没有 SAS 支持合同的 ACS 3.x 客户；包括 ACS 3.3 的次要升级版

1. 这里列出的仅仅是通过“详情垂询”的 URL 链接所能找到的所有产品的一小部分。有些产品设有一定的访问权限，或者无法通过分销渠道获得。经销商：要想获得最新的产品编号和订购信息，请访问分销产品查阅指南，网址是 <http://www.cisco.com/dprg>（目前只限于部分国家）。

详情垂询

请访问 Cisco Secure ACS for Windows 网站：<http://www.cisco.com/go/acs>

思科安全访问控制解决方案引擎

Cisco Secure ACS 解决方案引擎是一款高度安全、独立于 OS 的专用平台，提供了高度可管理的访问控制解决方案，进一步缩短了设置和排障时间。它提供了即插即用部署，一个高度可靠的验证、授权和记帐 (AAA) 解决方案，以及更高的总体拥有成本 (TCO) 保护。每个 Cisco Secure ACS 解决方案引擎都配有一个 Cisco Secure ACS 远程代理，可支持远程登陆和 Windows 验证。

适用场合

销售该产品

思科安全访问控制解决方案引擎

当客户需要以下这些特性时

- 需专用、增强安全、针对特定应用的设施包
- 凭借 Cisco Secure ACS 服务的整体可靠性和安全性，简化了日常管理
- 是不愿意在 Windows OS 上安装或管理 Cisco Secure ACS 的 Cisco Secure ACS UNIX 客户的合适替代品

关键特性

- 仅运行 Cisco Secure ACS 服务，以防止任何基于设备的 OS 更改、添加或配置修改
- 提供了一个串行控制台接口，以用于初始配置、随后对 IP 连接的管理、接入 Cisco Secure ACS HTML 接口，以及升级和恢复过程的应用
- 解决方案引擎专用管理工具提供了通用设施管理功能，包括备份、恢复、软件升级、监控、维护和排障功能
- 提供了针对 Windows 域的验证和远程用户帐户记录功能
- 分组过滤服务，可阻塞除必要的 Cisco Secure ACS 专用 TCP 和用户数据报协议端口外所有端口上的流量
- 事先安装的独立思科安全代理有助于保护 Cisco Secure ACS 解决方案引擎免遭“零日”攻击
- 内置 NTP 功能可保持网络时间同步及与其他 Cisco Secure ACS 应用或网络设备的一致性

产品特性

特性	思科安全访问控制解决方案引擎 ¹
处理器速度	Pentium IV, 3.2GHz
内存	1GB RAM
硬盘	80GB 磁盘空间
接口	2 个内置 10/100 以太网控制器和 1 个软驱

1. 专用于 Cisco ACS 解决方案引擎。其他特性可参见第 5-7 页，基于 Windows 的思科安全访问控制服务器

部分产品编号和订购信息¹

Cisco Secure ACS 解决方案引擎

CSACSE-1112-K9

CSACSE-1112-UP-K9

CSACSE-3.3-SWMR-K9

Cisco Secure ACS 3.3 解决方案, 包括硬件和软件

ACS 3.X 开放服务器或 1111 到带 ACS 3.3 的 Cisco 1112 的升级工具

CSACS 解决方案引擎软件 3.3-Jul04 的次要版本升级

1. 这里列出的仅仅是通过“详情垂询”的 URL 链接所能找到的所有产品的一小部分。有些产品设有一定的访问权限, 或者无法通过分销渠道获得。经销商: 要想获得最新的产品编号和订购信息, 请访问分销产品查阅指南, 网址是 <http://www.cisco.com/dprg> (目前只限于部分国家)。

详情垂询

请访问 Cisco Secure ACS 解决方案引擎网站:

<http://www.cisco.com/en/US/products/sw/secursw/ps5338/index.html>

思科安全用户注册工具

Cisco Secure URT 是一种虚拟局域网分配服务, 它可以主动地识别和验证用户, 并通过到 Cisco Catalyst 交换机网络的动态 VLAN 分配, 将他们与他们所需要的网络服务和资源相关联。URT v2.5 推出了很多创新的功能, 包括从 Windows、Macintosh 和 Linux 客户端进行基于 Web 的登陆, RADIUS 和轻型目录接入协议 (LDAP) 认证, 以及客户端和虚拟局域网策略服务器 (VPS) 之间的安全连接。它还包含一种基于介质访问控制 (MAC) 地址的安全功能, 使得用户只有在使用经过授权的机器时才能接入网络。基于 Web 的 LAN 验证可以在 LAN 环境中为用户提供移动能力。

适用场合

销售该产品

思科安全用户注册工具 (URT)

当客户需要以下这些特性时

- 可以在 Windows、Macintosh 和 Linux 客户端平台上进行基于 Web 的 LAN 验证——适用于 LAN 环境中的移动用户
- 通过基于 MAC 的安全选项加强安全性, 禁止用户从没有注册的 PC 上登陆 VLAN
- RADIUS 身份验证和记帐支持
- 每个端口支持多个用户权限

关键特性

- Web 客户端登陆界面——可以为 Windows、Macintosh 和 Linux 客户端平台提供可定制的、基于 Web 的身份验证
- 基于 MAC 的安全选项——提供增强的安全性, 禁止用户从没有注册的 PC 上登陆 VLAN
- RADIUS 身份验证和记帐支持——为 Web 登陆提供 RADIUS 身份验证
- 在 Cisco Secure URT 客户端和 VPS 服务器之间建立安全连接——URT v2.5 中添加了安全身份验证和数据加密功能, 可以为用户提供更加安全的连接
- LDAP 支持 (活跃目录和 NDS 目录)——Cisco Secure URT v2.5 支持 Windows 的活跃目录和 Novell 的 NDS LDAP 服务器
- 每个端口多个用户——旧版本的 Cisco Secure URT 在一个端口上只能支持一个用户登陆
- Windows NT 群组显示——增强的 URT 管理员界面可以显示属于一个 Windows NT 群组的用户
- MAC 地址事件历史——利用 URT v2.5 的基于 MAC 地址的登陆/退出, 可以将事件作为一个选项添加, 并报告到历史事件工具

产品特性

特性	Cisco 安全用户注册工具 (URT)
服务器要求	Windows 2000 (SP2) Server, Professional, Windows XP Professional – 最低硬件要求 (Pentium III, 512MB DRAM, 65MB 磁盘空间)
用于 Web 登陆的浏览器	Netscape 4.79 和 6.2 版; IE 5.5 版 (SP2) 或者 6.0 版
客户端软件要求	Windows 98 (2ndE), Windows NT 4 Workstation/Server (SP6A), Windows 2000 (SP2) Professional/Server, Windows XP Professional, Windows XP Home (仅限 Web 客户端), Mac OS 10.1 (仅限 Web 客户端), Linux Redhat/SuSE/Mandrake/VA (仅限 Web 客户端) —— Web 客户端最低硬件要求 (Pentium II, 256MB DRAM, 65MB 磁盘空间), 传统客户端最低硬件要求 (Pentium II, 64MB DRAM, 1MB 磁盘空间)
支持的思科产品 (最新测试的版本)	1900 系列 (1912, 1924), v.9.00.05; C2800 系列 (2822, 2828), v.9.00.05; C2900XL 系列 (2908XL, 2916XL, 2912XL, 2912LRE-XL, 2924XL, 2924LRE-XL), v12.0 (5) WC3b; C2948GL3 系列 (2948GL3, 4232), v12.0 (18) W5 (22b); C2950 系列, v12.1.6EA2c; v12.0 (5) WC3b; C3550 系列, v12.1.8.EA1c; C4000 系列 (4003, 4006, 4912g), v7.1 (2); C5000 系列 (2900, 2926, 2948, 5000, 5002, 5500, 5505, 5509); C6000 系列 (6006, 6009, 6506, 6509, 6513) v7.1 (3)

部分产品编号和订购信息¹

思科安全用户注册工具 (URT)

CSURT-1102-K9

启动工具包: 包括一 (1) 个用户注册工具 2.5 软件使用许可和一 (1) 个 Cisco 1102VLAN 策略服务器 (VPS) 设备

URT-1102-HW-K9

纯硬件; Cisco 1102 VP 设备; 其他备份设备, 用于分布式部署或者需要 Web 登陆功能的部署

CSURT-2.5-SWMR-K9

次要版本升级工具, 用于没有 SAS 支持合同的 URT 2.x 客户; 包括 URT 2.5 的次要升级版

1. 这里列出的仅仅是通过“详情垂询”的 URL 链接所能找到的所有产品的一小部分。有些产品设有一定的访问权限, 或者无法通过分销渠道获得。

详情垂询

请访问思科安全用户注册工具网站: <http://www.cisco.com/go/urt>

Cisco IOS 防火墙

Cisco IOS 防火墙功能集为每一个网络周边集成了强大的防火墙功能和入侵检测, 丰富了 Cisco IOS 软件的安全功能。如果与 Cisco IOS IPSec 软件和其他基于 Cisco IOS 软件的技术 (例如 L2TP 隧道和服务质量[QoS]) 相结合, 它可以提供一个全面、集成的虚拟专用网解决方案。因为它可以用于多种思科路由器, 所以它让客户能灵活地选择一个符合其带宽、LAN/WAN 密度和多服务需求的解决方案, 同时获得先进的安全性。

适用场合

销售该产品

Cisco IOS 防火墙

当客户需要以下这些特性时

- 一个可以在同一个平台上提供强大的安全性和多协议路由功能的集成状态化防火墙解决方案
- 从 Cisco 800 到 Cisco 7500 和 Catalyst 6000 的可扩展选项
- 利用现有基础设施的低成本解决方案
- 可以为分支机构和远程机构提供安全的外部网、内部网周边和互联网连接
- 通过基于 Cisco IOS 软件的 VPN 解决方案提供安全的远程接入或数据传输
- 实时 (内置) 的集成化 Cisco IOS 入侵防御系统 (IDS), 可以补充防火墙或现有的 IDS (Cisco Secure IDS) 解决方案
- 在单个用户的基础上提供安全和网络接入

关键特性

- 基于上下文的访问控制（CBAC）可以提供安全、状态化的、基于应用的分组过滤，支持最新的协议和先进的应用
- Cisco IOS 内置的入侵检测功能，可以根据 740 多种攻击特征实时地监控、侦听并对网络滥用作出响应
- 支持通过专用域在路由器上的本地 URL 过滤和利用外部 Websense 及 N2H2 服务器进行的 URL 过滤
- 动态的单用户验证和授权，适用于 LAN、WAN 和 VPN 客户
- 为 https、ftp 和 telnet 连接提供验证代理
- 支持思科路由器和安全设备管理器（SDM）
- 通过使用 VPN/ 安全管理解决方案（VMS）和 IP Solution Center（ISC）进行图形化配置和管理
- 为一个完整的、基于 Cisco IOS 软件的 VPN 解决方案提供强大的周边安全，其中包括 IPSec、QoS 和隧道

产品特性

特性	Cisco IOS 防火墙
所支持的网络接口	支持平台上的所有网络接口
支持的平台	Cisco 1720、1800、2600/2600XM、2800、3700、3800、7100、7200 和 7301 系列路由器平台（支持全部功能集） Cisco 800、UBR900、1600 和 2500 系列路由器平台，包括除入侵检测/防御和验证代理之外的所有防火墙功能
同步进程数	没有最大限制，具体取决于平台、网络连接和流量
Cisco IOS Firewall 性能	C800-10Mbps，C1700: 20Mbps；Cisco 1800: 125 Mbps，C2600XM: 35Mbps；C2691-VPN: 197Mbps；Cisco 2800: 530Mbps；C3725-VPN，C3745-VPN: 197 Mbps；Cisco 3825: 855Mbps；Cisco 3845:1 Gbps，7200/7301 捆绑: 1Gbps

部分产品编号和订购信息

要了解包含防火墙（FW）和入侵防范（IPS）功能的 Cisco IOS 软件镜像的信息，请查看所支持的各个平台所在页，以及 Cisco IOS 功能浏览器，请访问 <http://www.cisco.com/go/fn>（需要 CCO 注册），查看相关产品编号和更多信息。

详情垂询

请访问 Cisco IOS 防火墙特性集网站：<http://www.cisco.com/go/firewall>