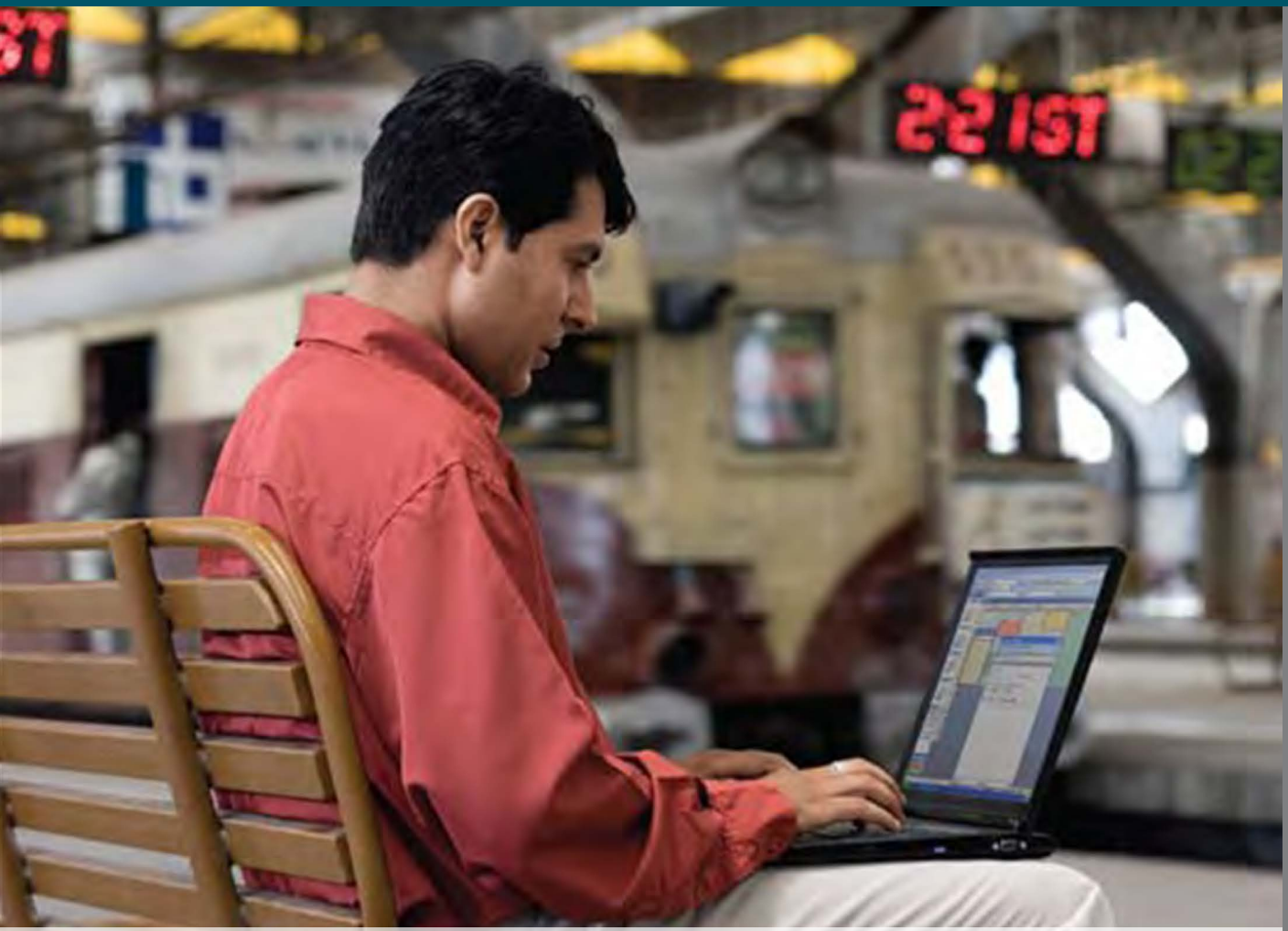
快速参考指南
供客户阅读

思科®安全解决方案



2009 年 1 月

目录

退出

为什么安全比以往任何时候都重要

首页

维护声誉

当今世界充满安全挑战，企业面临诸多风险。一次数据泄露就可能断送您在客户、投资者和市场中的良好声誉。

满足合规性要求

每家公司都应遵守一定的规章制度，内容通常与隐私与客户信息保护有关。合规性可确保坚实可靠且全面的安全性。

保护商业信息

信息是所有企业的核心所在。重要资产无论位于何处，其可用性、完整性和机密可靠性均应得到保护。

优化业务运营

大多数公司很难确定停机一天的成本，因为需要考虑诸多的直接与间接因素，其中包括生产力损失、业务和客户忠诚度损失、对声誉及品牌形象的影响、维修及恢复成本，以及潜在的法律责任。

思科® 自防御网络

有些企业既需要降低安全及合规性方面的 IT 风险，又要降低 IT 管理负担与总拥有成本，对此，思科可通过系统方法提供领先的安全保证。与其它安全供应商不同，思科将同类最佳方法与系统方法有机结合，从而为客户带来众多优势：

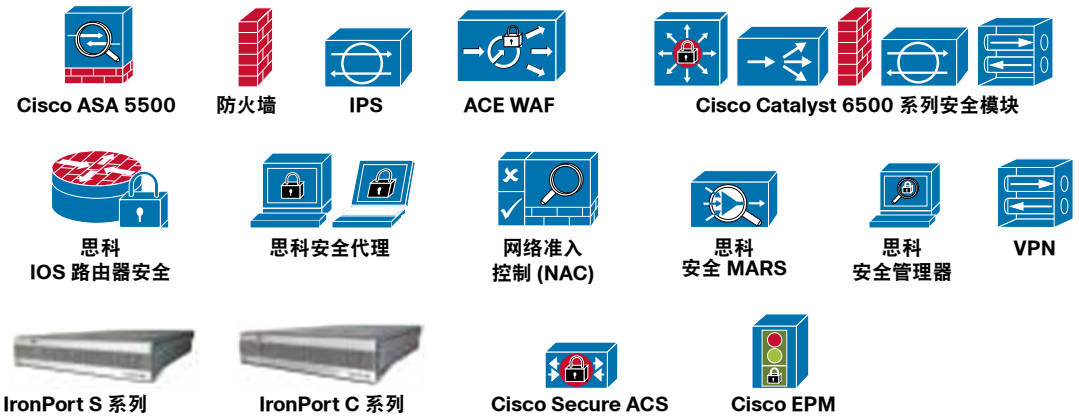
- 采用同类最佳的安全方案解决可能出现的安全威胁
- 采用系统方法解决各种无所不在的威胁，力求满足合规性要求，同时提高管理成本效益
- 1995 年至今的安全领域创新历史
- 在防火墙技术、虚拟专用网、电邮与 Web 安全以及入侵防御方面，处于网络安全市场领先地位
- 屡获殊荣的产品系列
- 历经客户验证，拥有多个成功案例

为什么选择思科?

思科提供迄今为止最为广泛和深入的产品系列及服务组合，并授权我们的合作伙伴按照您的独特需求设计及实施个性化解决方案。

有关详情，请访问：
http://www.cisco.com/go/securitysolutions

思科安全解决方案一览。



目录

退出

Cisco ASA 5500 系列自适应安全设备

概述

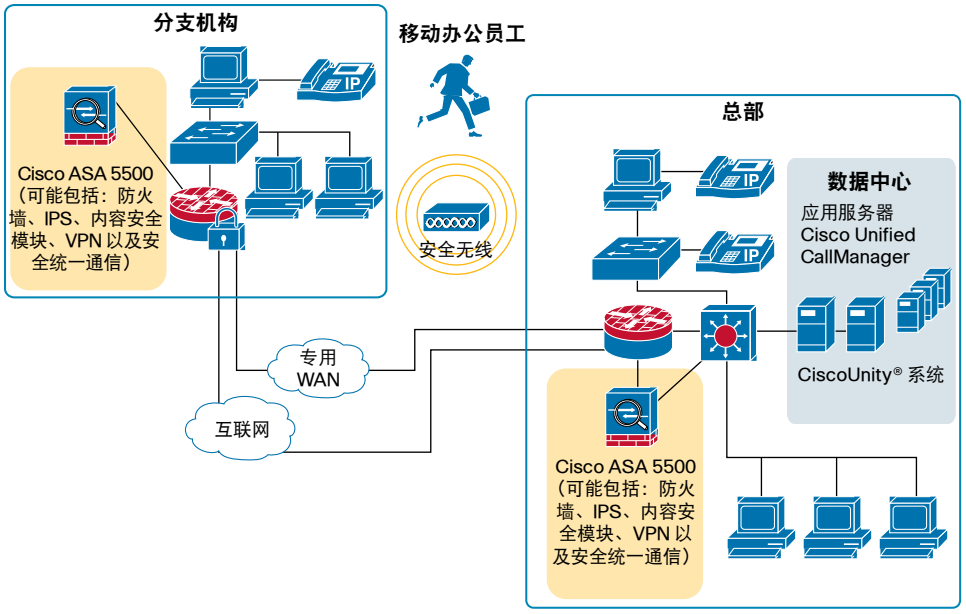
- Cisco® ASA 5500 系列将多功能、高性能防火墙（包括应用防火墙服务）、入侵防御、内容安全、IPsec/SSL VPN，以及安全统一通信技术汇聚到简便易用的单一安全设备中
- 现在，您可以将多项安全功能整合到一台高性能设备中，来降低成本与复杂性，为您的网络提供工业级强度的安全保障
- Cisco ASA 5500 系列集成安全平台可以灵活扩展，满足各种不同规模企业的安全需求

好处

- 将防火墙、SSL 与 IPsec VPN、入侵防御、网络内容安全服务以及安全统一通信技术集成到单一硬件平台，降低了成本和复杂性
- 提供多种高性能安全服务，成本仅与单一防火墙相当
- 可应对新的安全威胁
- 具有全面的远程办公保护功能，为远程工作者提供数据及语音保护
- 仅用一台设备即可提供综合威胁保护解决方案，适用于 SSL 与 IPsec VPN 连接

有关详情，请访问：
http://www.cisco.com/go/asa

Cisco ASA 5500 系列自适应安全设备在网络中的应用。



目录

退出

防火墙

首页

概述

防火墙可以保护专用网络的各种资源，防止内部或外部用户未经授权访问应用、网络和数据。

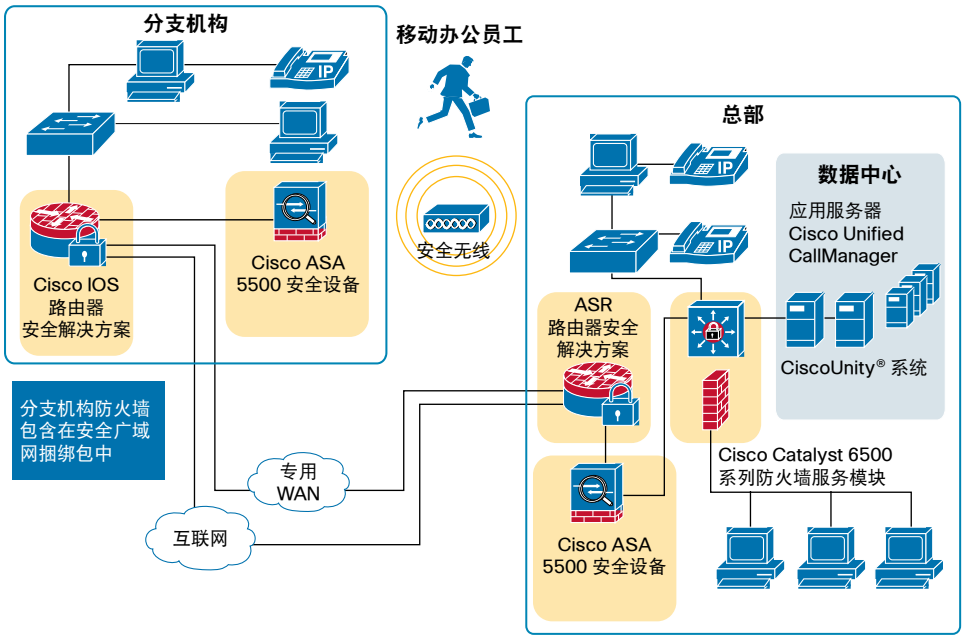
- 思科® 防火墙解决方案提供集成的网络安全服务，包括：
  - 状态包检测
  - 应用层及协议检测
  - 内部入侵防御
  - 丰富的多媒体及语音安全
- 思科提供多种防火墙解决方案，包括：
  - Cisco Catalyst® 6500 系列防火墙服务模块 (FWSM) 适用于对扩展性要求更高的环境
  - Cisco ASA 5500 系列自适应安全设备
  - 思科路由器上的基于 Cisco IOS® 软件和 Cisco NX-OS® 软件的防火墙

好处

- 可为任何规模企业的重要网络提供保护，防止未经授权的访问
- 具备先进的应用检测能力，可保护应用及网络服务免受攻击
- 支持多协议动态路由，提高了网络可靠性及性能
- 使用思科安全管理器可以集中管理所有防火墙解决方案
- 提供恢复力极强的低间断安全基础设施
- 最大限度地增加网络运行时间，提高生产率
- 可安全部署下一代统一通信及多媒体应用

有关详情，请访问：
http://www.cisco.com/go/firewall

思科防火墙解决方案在网络中的应用。



目录

退出

入侵防御系统 (IPS)

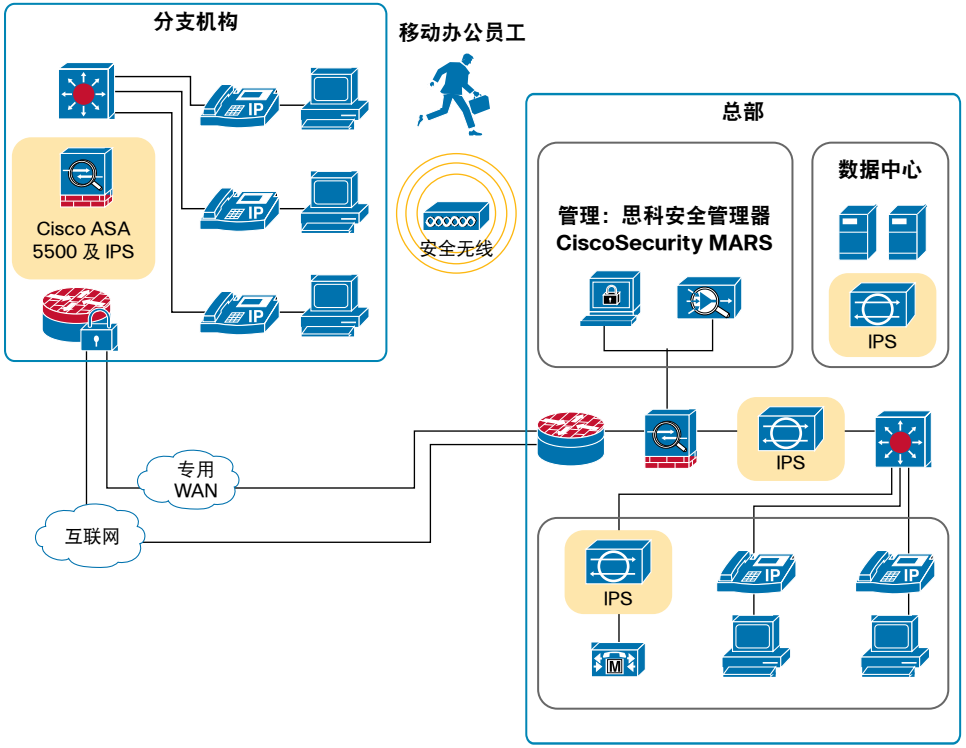
首页

概述

思科入侵防御系统 (IPS) 是全世界最值得信赖、广泛部署的 IPS，针对 3 万多种威胁提供久经验证的保护，帮助客户保护机密数据，满足不断增长的合规性要求。思科 IPS 可对包括蠕虫、间谍软件/广告软件、网络病毒和应用滥用等恶意流量提前进行准确检测、分类并阻止其入侵，保证业务的连续性。思科流量异常检测器可以在签名更新前阻止零日攻击。

思科 IPS 可与其他关键网络组件配合使用，提供全面的端到端网络保护。思科 IPS 会与基于主机的 IPS（思科安全代理）和思科无线控制器共享各类威胁信息。作为专用设备，思科 IPS 也可集成至思科防火墙、交换机及路由器平台，实现最大程度保护以及部署灵活性。

思科 IPS 产品在网络中的应用。



目录

退出

入侵防御系统 (IPS)（续）

好处

- 依托 12 年 IPS 创新经验打造的先进 IPS 技术
- 针对 3 万多种威胁提供久经验证的保
- 与基于主机的 IPS（思科安全代理）紧密集成，提供端到端保护
- 与思科无线控制器紧密集成，提供安全的无线部署
- Cisco IPS Manager Express 适用于小型企业，可简化企业管理
- 思科安全管理器和思科安全监控、分析及响应系统（思科安全 MARS）提供企业级策略管理
- 除了防止病毒爆发以外，还提供诸多其他保护，如针对公司信息的攻击
- 帮助防止因服务器遭受入侵引起的崩溃、窃取或篡改所带来的严重损失
- 在网络层面阻止蠕虫和病毒爆发，将其控制在用户桌面之外

灵活的部署选项包括：

- Cisco IPS 4200 系列传感器可作为独立的 IPS 设备使用。要了解详情，请访问：http://www.cisco.com/go/4200
- 集成的 Cisco ASA 5500 系列高级检测及防御安全服务模块（AIP SSM10、AIP SSM20 与 AIP SSM40），通过易于部署的单一平台提供入侵防御、防火墙及 VPN 等诸多服务。要了解详情，请访问：http://www.cisco.com/go/aipssm
- Cisco AIM-IPS、NME-IPS 或 Cisco IPS 传感器软件适用于集成服务路由器。要了解详情，请访问：http://www.cisco.com/go/ime
- Cisco Catalyst 6500 系列入侵检测系统 (IDSM-2) 模块。要了解详情，请访问：http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html
- 思科自适应无线 IPS 可保护无线信号免受入侵者劫持，同时思科网络 IPS 可防止经过身份验证的用户（拥有合法用户名和密码）进行恶意或未经授权的活动，如窃取机密数据等。要了解详情，请访问：http://www.cisco.com/go/wips

有关 Cisco IPS 解决方案的详细信息，请访问：
http://www.cisco.com/go/ips

目录

退出

思科路由器安全解决方案

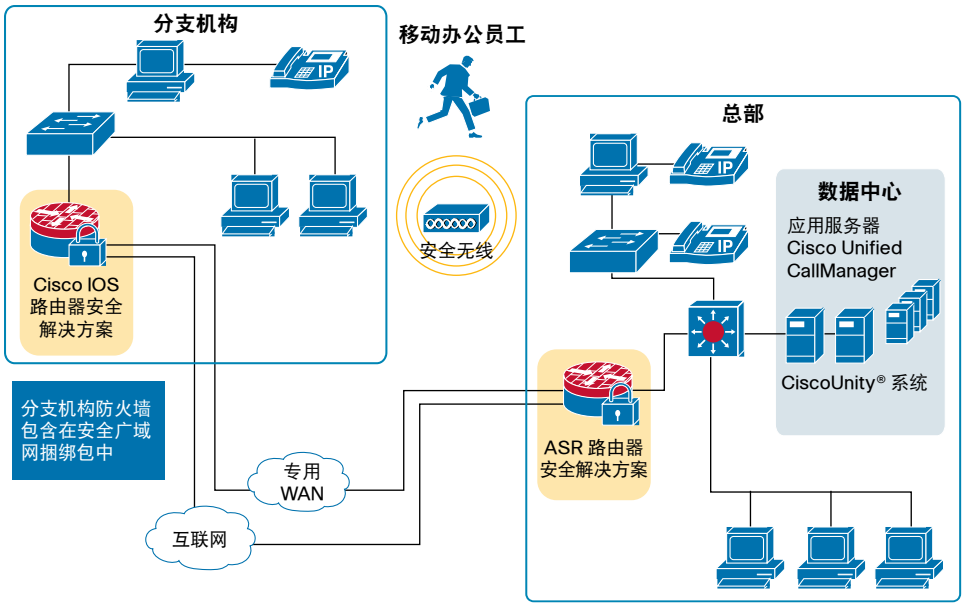
首页

概述

保护重要网络基础设施（包括思科® 路由器）至关重要。

- 思科路由器安全解决方案增加了重要的安全功能，极大地提高了您的投资回报率 (ROI)。
- 此功能集为您的分支路由器添加了以下功能：站点到站点 VPN、IPsec 与 SSL 远程访问 VPN、经 Common Criteria/EAL4 认证的状态防火墙、内容过滤、内部入侵防御、网络准入控制 (NAC) 以及安全管理。
- 良好的业务连续性设计通常包括加密的双 WAN 链接、灾难期间的远程网络访问、以及针对关键服务的带状态故障切换。思科路由器安全解决方案可以实现所有这些解决方案。
- 思科路由器安全解决方案还支持其它的网络服务，例如安全统一通信（语音和视频）和安全无线 LAN。

思科路由器安全解决方案在网络中的应用。



目录

退出

思科路由器安全解决方案（续）

首页

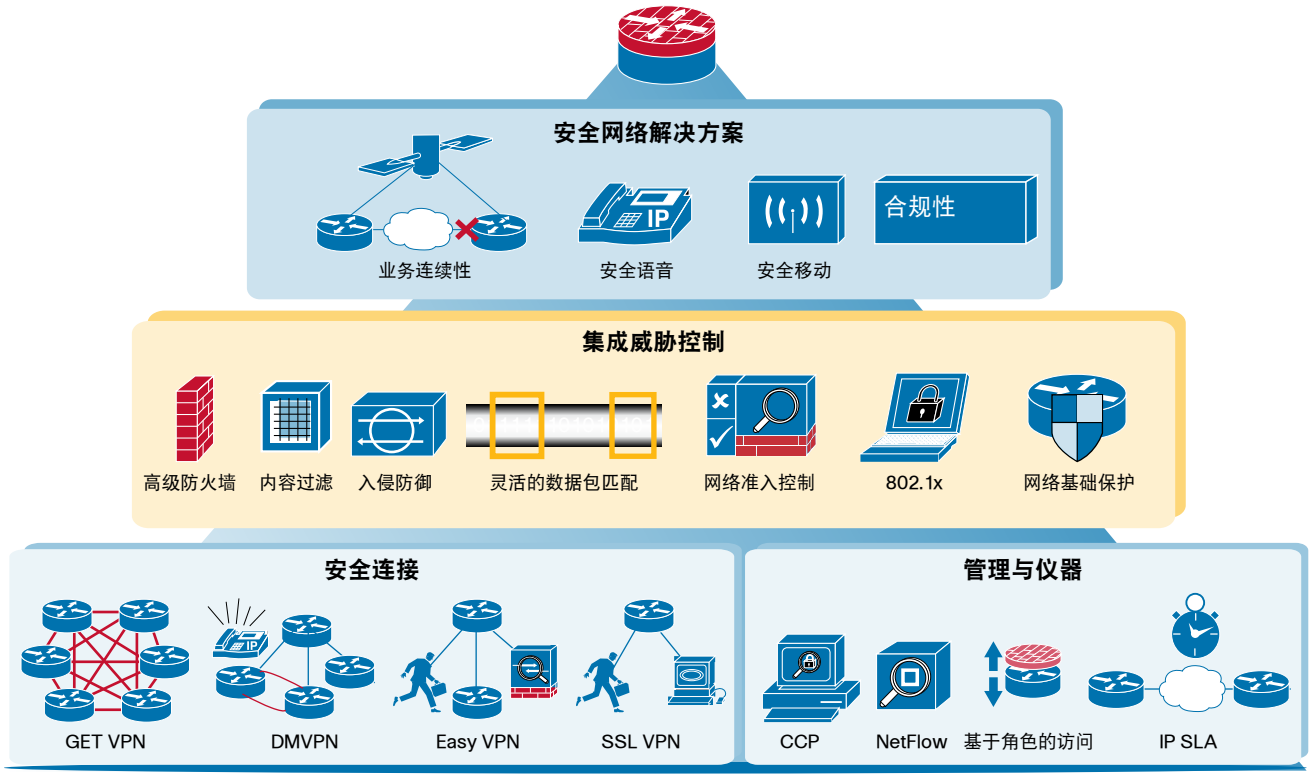
好处

- 通过增加如防火墙、IPsec 与 SSL VPN、入侵防御、内容过滤，以及网络准入控制 (NAC) 等安全服务项目，大幅提升路由器价值，实现投资回报最大化
- 帮助企业安全部署无线 LAN 和统一通信服务，例如语音和视频服务
- 提供安全可靠、高性价比、易于管理且随意扩展的解决方案，实现站点到站点业务通信
- 符合美国 联邦及各州的数据和网络隐私法律（如支付卡行业 [PCI] 规定）要求
- 将安全及其他服务整合到单一网络设备中，减轻了管理负担

有关详情，请访问：

http://www.cisco.com/go/routersecurity

思科路由器安全解决方案可提供的安全服务



目录

退出

端点安全

首页

思科安全代理

概述

思科® 安全代理 (CSA) 是首个终端安全解决方案，将“零更新”攻击保护、数据丢失防御以及基于签名的杀毒功能结合到单一的代理中。这种独特的功能组合可保护服务器和桌面免受复杂的零日攻击，确保在简单的管理基础设施中满足可接受的使用策略及遵从性策略要求。

- 您可以获得更好的安全性，节省安全预算：Cisco Security Agent 6.0 增加了杀毒功能，无需额外和续期费用。
- 思科安全代理 (CSA) 端点安全集成了数据丢失防御功能：采用单一的代理与管理控制台同时为端点完整性与机密数据提供保护
- 思科安全代理 (CSA) 提供经过认证的 PCI 保护。
- 思科安全代理 (CSA) 在端点保护方面处于业界领先水平，可有效防止针对性攻击、恶意移动代码、rootkit、蠕虫以及零日攻击。

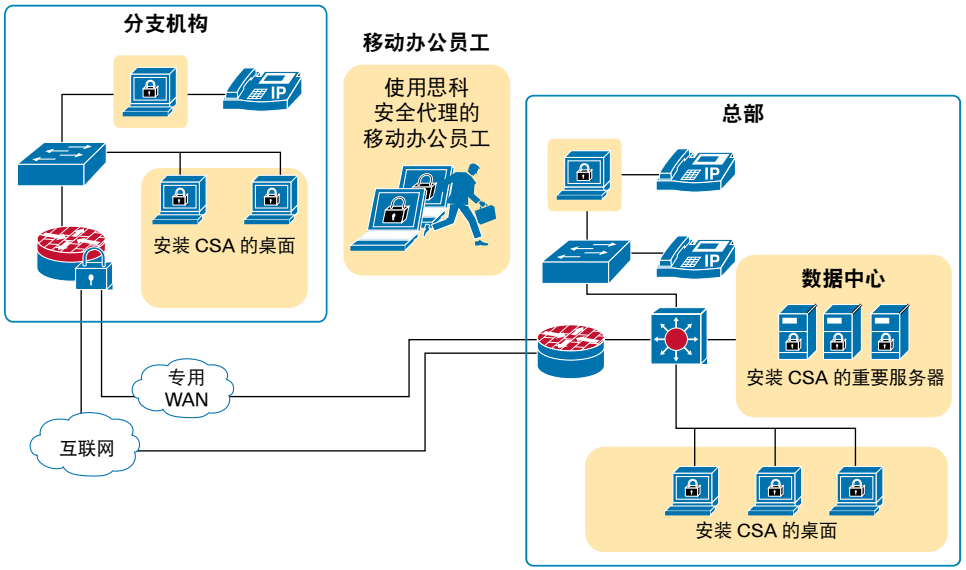
好处

- “零更新”保护可以减少针对漏洞报告的紧急修补，最大限度降低修补引起的停机时间与 IT 费用。
- 敏感数据的可见性及控制可以防止用户行为或针对性恶意软件造成的数据丢失。
- 预定义的遵从性策略及可接受的使用策略提高了活动管理、报告及审计的效率。
- “始终警惕”的安全防护意味着您的系统时刻处于保护状态，即使用户未接入公司网络或未安装最新补丁也不例外。

有关详情，请访问：

http://www.cisco.com/go/csa

思科安全代理 (CSA) 在网络中的应用。



目录

退出

端点安全

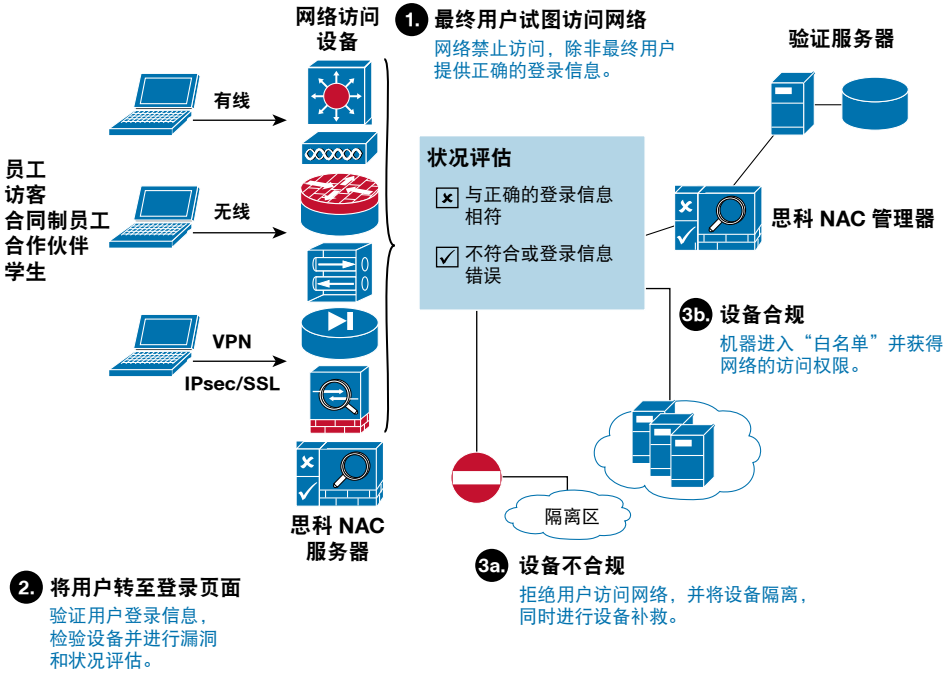
首页

思科网络准入控制 (NAC)

概述

- 思科® 网络准入控制 (NAC) 使网络能够对所有试图访问网络的设备实施安全策略。
- 思科 NAC 先确认用户身份，然后再准予其访问网络，以此来保护敏感数据，阻止未经授权的访问。
- 思科 NAC 可以最大程度地降低不合规设备带来的风险，且不受系统类型、所有权或访问方法限制，打造更加灵活、安全的网络环境。
- 不合规设备可通过隔离修复转变成合规设备。
- 可选 Cisco NAC Profiler 还可以自动检测并列出所有 LAN 连接端点，包括 IP 电话和打印机等非 PC 设备。它可以根据设备信息采取适当的思科 NAC 策略，从而简化 NAC 部署。
- 可选 Cisco NAC Guest Server 可支持整个客户访问生命周期（配置、通知、管理与报告）。

思科 NAC 在网络中的应用



目录

退出

思科网络准入控制 (NAC)（续）

好处

- 在网络层面实施安全策略合规性验证
- 提供主动保护，防止基础设施受到破坏（如病毒和蠕虫）
  - 控制并减少基础设施受到大规模破坏的机率
  - 降低运营费用，提高员工生产率
- 防止未经授权的访问
  - 控制基于用户和设备信息的网络访问，保证网络安全，保护机密信息
  - 有效控制客户访问及合作伙伴连接
- 提供全面完善的服务（用户身份验证、设备状态验证、策略实施、补救、设备分析、访客安全等），满足客户各种业务需求
- 设备分析服务可自动检测并记录设备，降低 IT 负担
- 访客服务可提供安全的访客接入，确保访客满意度
- 支持所有客户事例，包括园区、分支机构、无线网络以及 VPN
- 保证所有公司设备及非公司设备的安全
- 可部署于第 2 层或第 3 层、带内或带外
- 降低 IT 安全风险，满足合规性要求

有关详情，请访问：
http://www.cisco.com/go/nac

退出

电邮、Web 及内容安全

思科 Web 安全网关设备

概述

由网络流量引起的安全威胁数量繁多，肆虐成灾。传统的网关防御已不足以应对众多网络恶意软件的入侵，企业网络正面临这些威胁所带来的内在危险。

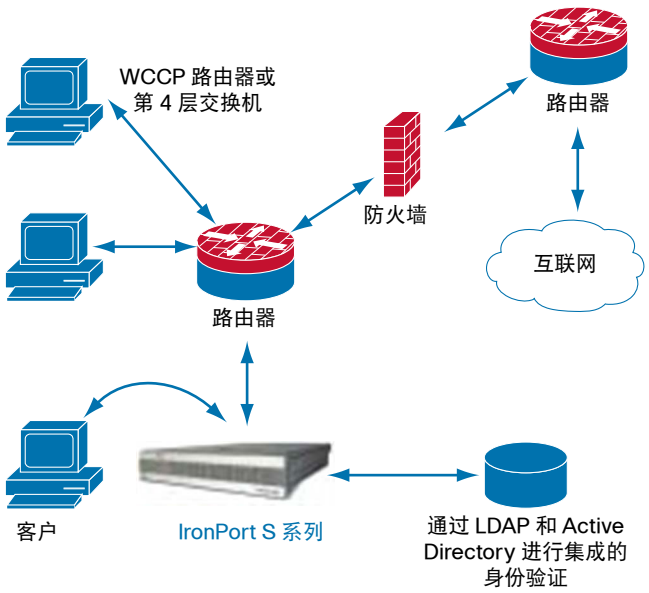
- 据估计，约 75% 的企业 PC 感染了间谍软件，但只有不到 10% 的企业部署了外围恶意软件防御措施。
- Cisco® IronPort® S 系列网络安全网关是业内首创，也是唯一将传统 URL 过滤、信誉过滤及恶意软件过滤整合于同一平台的设备。
- S 系列采用单一设备提供多层防护，同时又保持了运营商级的性能

好处

- Cisco IronPort S 系列提供单一设备解决方案，保护和控制企业网络面临的三大网络流量风险，即安全风险、资源风险与遵从性风险。
- Cisco IronPort S 系列可在网络外围阻止恶意软件威胁，从而大幅降低企业的管理成本、防止攻击者的网络“回拨”活动、减少客服电话、提高效率、并消除这些威胁带来的业务风险。
- 业界首个网络信誉过滤器，提供强大的外层防御。Cisco IronPort 网络信誉过滤器采用 SenderBase 技术分析 50 多种不同网络流量及相关网络参数，可准确评估网址的可信度。
- 通过采取适当的使用策略，企业不仅可以监控网络活动，还可以帮助员工充分认识和了解这些策略所减轻的风险。
- 不同于其它需要多个硬件维护的 ICAP 解决方案，Cisco IronPort S 系列只需一个平台即可实现全面、深入的防御。
- 为最大限度地降低管理费用，Cisco IronPort S 系列配备了直观的图形用户界面，易于安装和管理，支持自动更新，并提供全面的监测与报警功能。
- Cisco IronPort S 系列提供实时及历史安全信息，使管理员能及时掌握网络流量活动情况。

有关详情，请访问：
http:// www.ironport.com/web

Cisco IronPort S 系列在网络中的应用。



目录

退出

电邮、Web 及内容安全

首页

思科 IronPort 电邮安全设备

概述

思科提供了世界上最强大的多层方法确保电邮安全。Cisco® IronPort® C 系列提供世界一流的垃圾邮件防护、数据丢失保护、防病毒爆发过滤器、以及基于签名的反应过滤器，同时还结合了内容过滤及同类最佳的加密技术，为客户构建迄今为止最高级别的电邮安全防护体系。

目前，邮件传播的威胁包括病毒攻击、垃圾邮件、误报、分布式拒绝服务 (DDoS) 攻击、间谍软件、网络钓鱼（欺诈）、违规和数据丢失。Cisco IronPort 电邮安全设备具备无可比拟的出色性能，采用简便易用的单一设备提供业界领先的保护措施，可有效防止垃圾邮件和病毒攻击以及数据丢失等。

好处

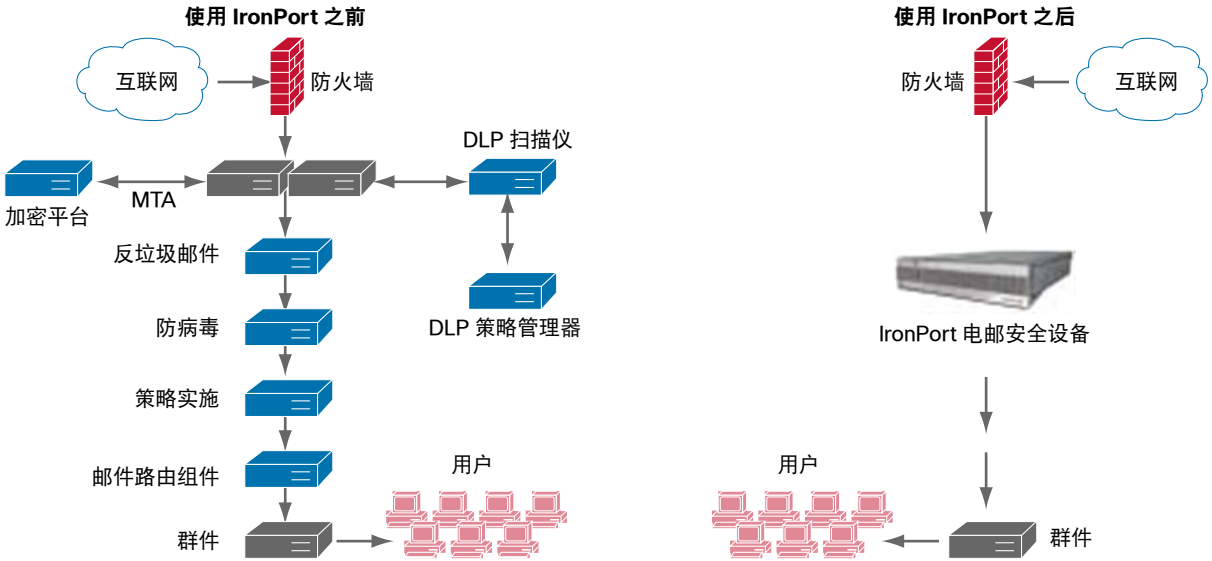
Cisco IronPort 的反垃圾邮件解决方案可以快速、准确地防止垃圾邮件爆发，为客户提供安全保障。

- Cisco IronPort 将 SenderBase 过滤器与内容级分析和 Cisco IronPort 反垃圾邮件技术完美结合，为客户提供业界最佳的安全保障：可阻止 99% 的垃圾邮件，误报率几乎为零。
- Cisco IronPort C 系列将邮件操作和安全防护整合到同一平台，显著降低了总体拥有成本 (TCO)。C 系列拥有无与伦比的性能，C 系列提供拨号音可用性，在流量高峰期节省数小时的工作时间和数千美元。
- Cisco IronPort 可向系统管理员提供必要的信息，利于重要安全决策，实现投资回报率。

有关详情，请访问：

http:// www.ironport.com/email

Cisco IronPort 在网络中的应用。



目录

退出

电邮、Web 及内容安全

首页

Cisco ACE Web 应用防火墙

概述

许多公司都希望通过新型 Web 2.0 应用与服务项目来提高效率，增加收益。然而，这些新应用往往是定制型应用，安全性能欠佳。

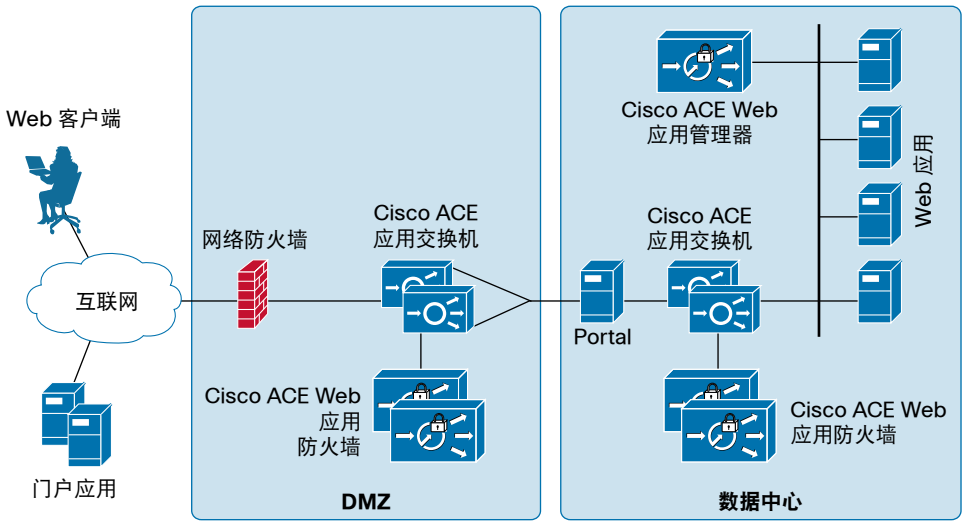
- Cisco® ACE Web 应用防火墙将深度 Web 应用分析与高性能可扩展标记语言 (XML) 检测与管理完美结合，可以全方位防止针对 Web 应用的各种威胁，包括身份盗用、数据窃取、信息泄露、应用崩溃、欺诈以及针对性攻击。
- Cisco ACE Web 应用防火墙可帮助企业存储、处理及传输信用卡数据，满足当前支付卡行业 (PCI) 数据安全标准 (DSS) 要求。
- Cisco ACE Web 应用防火墙别出心裁地将 HTML 和 XML 安全性有机结合，完全符合 PCI DSS 第 6.5 和 6.6 节关于强制实施 Web 应用防火墙的要求。

好处

- 符合 PCI DSS 标准要求，可根据客户需求定制专用的 PCI 策略，并针对 Web 应用活动提供保护、审计与报告
- 提供全代理安全保障，同时适用于传统 HTML Web 应用和新型 XML Web 服务应用
- 实施验证和授权，阻止未经授权的访问
- 在管理大型数据中心 XML 应用流量方面具备业界最佳的可扩展能力
- 实施积极与消极的安全措施，防止异常流量模式，识别并仅允许正常流量
- 提供企业级用户友好管理，可随时随地通过 Web GUI 进行访问

有关详情，请访问：
http://www.cisco.com/go/waf

Cisco ACE Web 应用防火墙在网络中的应用。



目录

退出

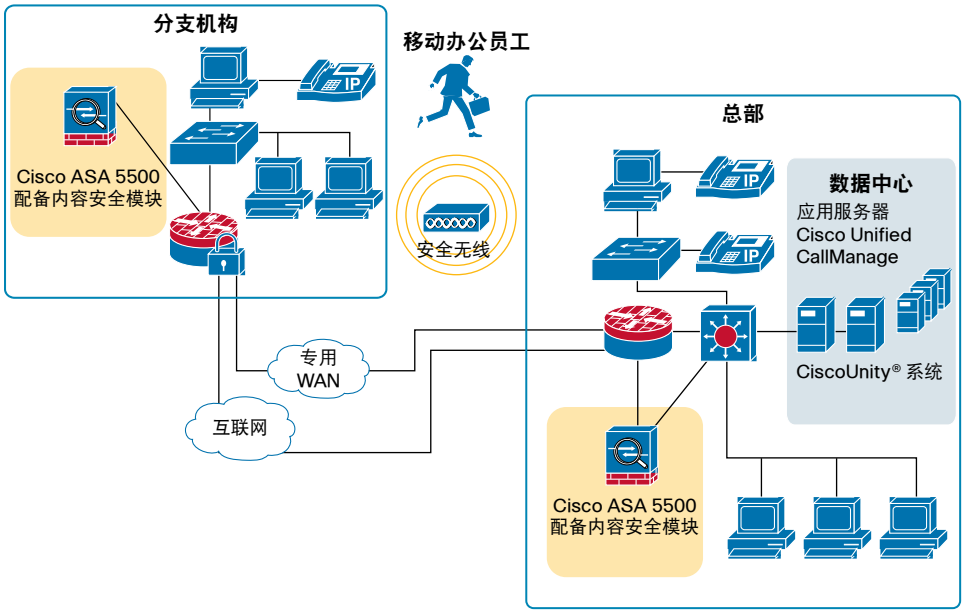
电邮、Web 及内容安全

Cisco ASA 5500 系列的内容安全

概述

- Cisco® ASA 5500 系列自适应安全设备配备内容安全与控制安全服务模块 (CSC-SSM)，是一体化威胁防御设备，融合了思科在防火墙和 VPN 方面的领先科技以及趋势科技公司在反恶意软件和网关内容安全方面的技术专长。
- 网络与安全管理员利用配备了 CSC-SSM 模块的 Cisco ASA 5500 系列，可以对包括蠕虫、间谍软件/广告软件、网络病毒和应用滥用等在内的恶意流量提前进行准确检测、分类并阻止其入侵，保证业务的连续性。
- 使用网关进行内容过滤可为公司及访客电脑提供同一层次的内容保护，与这些电脑所用的防病毒类型和状态无关。CSC-SSM 提供一整套综合的内容安全服务，除了防病毒服务外，还包括防垃圾邮件、网址过滤与阻止、防网络钓鱼以及防间谍软件服务。

思科内容安全解决方案在网络中的应用。



目录

退出

电邮、Web 及内容安全

Cisco ASA 5500 系列的内容安全（续）

好处

- Cisco ASA 5500 配备 CSC-SSM 模块，是多功能一体化设备，不仅具有防火墙与 VPN 安全技术，还可与部分远程办公室依然在用的思科 VPN 集线器和 Cisco PIX® 防火墙实现交互操作。
- 与单独的解决方案相比，该一体化设备可以最大限度降低日常管理成本，提高运营效率。
- 除防火墙与 VPN 安全防护外，该设备还提供网址和电邮过滤保护，使其免受病毒、垃圾邮件、间谍软件和钓鱼软件的攻击。
- CSC-SSM 模块具有全面、深入、便捷、易用的功能，包括防病毒、防垃圾邮件、防网络钓鱼、防间谍软件功能，以及网址和电邮过滤等。
- CSC-SSM 包括可随意配置的垃圾邮件过滤器。电邮信誉功能可向垃圾邮件发送者和僵尸网络的 IP 地址分配信誉分值，从而实时提供他们的信息。来自可疑 IP 地址的电邮在到达公司网络前会“在云端”被自动阻止。该级别的域名定制功能可让公司加强对电邮流量的控制，有助于节约内部网络的带宽。
- 网关、桌面、服务器以及电邮均可得到保护，90% 的垃圾邮件受到阻止，往来于信誉不佳站点的流量也得以阻断。
- 无关的内容不再干扰网络或系统。带宽和存储不再被垃圾邮件所占据。
- CSC-SSM 解决方案维护成本很低，安装完成后即可自动更新和过滤。

有关详情，请访问：
http://www.cisco.com/go/cscssm

目录

退出

思科安全监控、分析和响应系统 (MARS)

概述

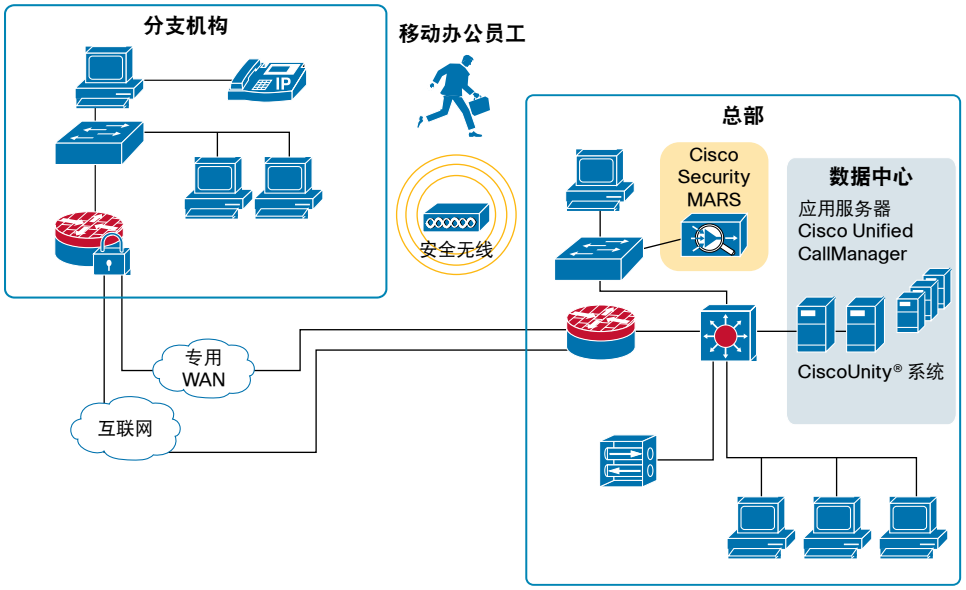
- 思科® 安全监控、分析和响应系统 (Cisco Security MARS) 包括一系列用于威胁管理、监控和防御的高性能可扩展设备。思科安全 MARS 有助于客户增强安全防护，提高网络及安全设备的使用效率。
- 思科安全 MARS 将传统的安全事件监控功能和网络智能融为一体，可对攻击、入侵及其他网络威胁做出实时响应，提供精确的智能防御。

好处

- 收集、分析及关联多种思科设备的数据
- 采用拓扑意识图形化显示攻击路径
- 提供防御建议，迅速遏制威胁
- 提供思科安全管理器链接，方便策略设置及事件查询
- 优化了 Cisco ASA 和 Cisco IPS 的故障排除
- 具备高性能：一台思科安全 MARS 设备每秒可处理 15,000 个事件

有关详情，请访问：
http://www.cisco.com/go/mars

思科安全 MARS 在网络中的应用。



目录

退出

思科安全管理器

概述

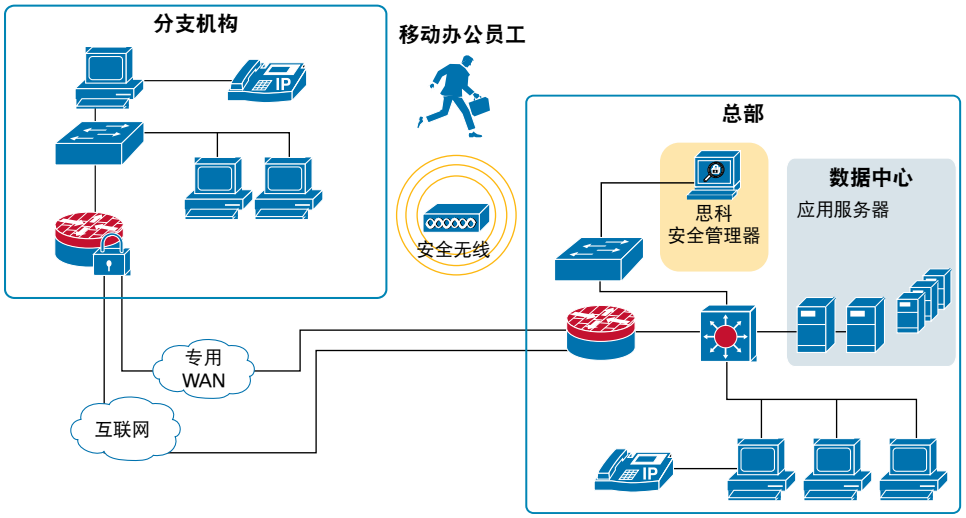
- 思科® 安全管理器是一款功能强大而又方便易用的解决方案，可为思科防火墙、VPN 和入侵防御系统 (IPS) 集中调配各种设备配置及安全策略。
- 思科安全管理器作为集中安全管理解决方案，部署更快、配置更为精确。
- 该解决方案可有效管理 10 台设备以下的小型网络，经扩展后，也可有效管理拥有数千台设备的大型网络。

好处

- 提供单一集成应用，用于管理思科安全设备与模块、路由器及交换机上的防火墙、VPN 和 IPS 安全服务
- 减少运营开支，同时提高设备配置的准确性与一致性
- 与思科安全 MARS 配合使用，可构建集安全配置、事件监控、威胁检测与防御于一身的综合安全管理解决方案
- 对威胁的响应速度更快 — 只需简单几步即可为数千台设备定义并分配全新的安全策略
- 拥有丰富的图形用户界面，使用极为方便
- 支持真正的企业级运营环境，并且支持多个安全管理员精细控制访问权限；可选的“工作流程”模式使安全和网络运营人员可以高效协作、各司其职
- 可对思科路由器、交换机与安全平台进行配置

有关详情，请访问：
http://www.cisco.com/en/US/products/ps6498/index.html

下图显示思科安全管理器如何融入网络中。



目录

退出

思科安全访问控制系统 (ACS)

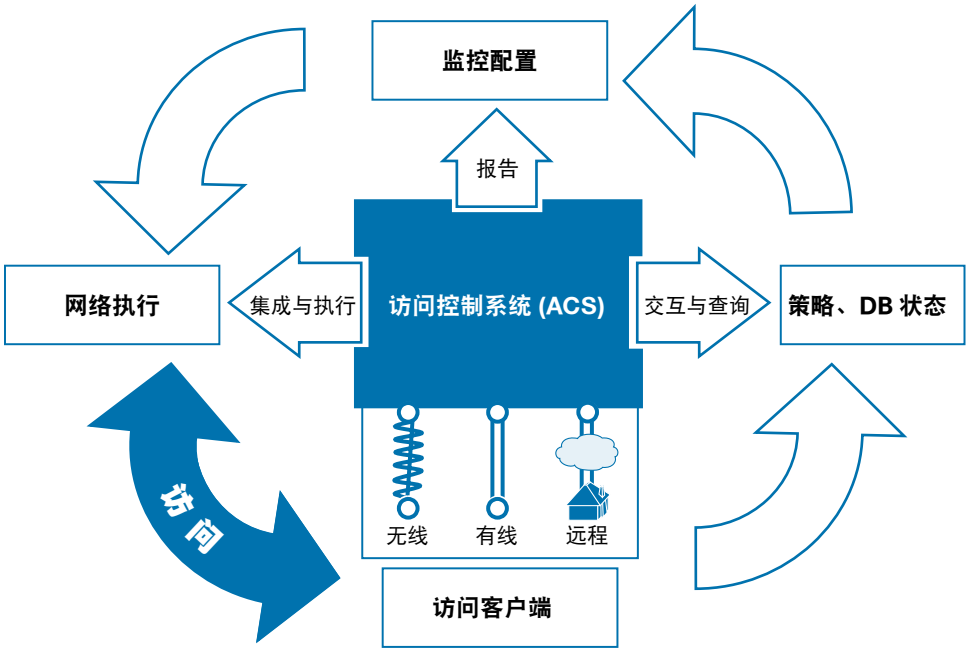
概述

- 思科® 安全 ACS 是全球最值得信赖的企业网络访问策略和身份识别系统，全球企业用户超过 4 万家。
- 思科® 安全 ACS 性能强大、功能丰富，是几乎所有网络身份验证和访问策略不可或缺的组成部分。
- 思科® 安全 ACS 可作为管理网络访问策略的控制点，与外部数据库、策略服务器和状态引擎进行交互通信。
- 思科® 安全 ACS 可以更好地控制、监控、实施对公司资源的访问，满足不断变化的业务及法规需求。

好处

- 集中控制网络访问与设备管理。
- 可用于几乎任何支持 RADIUS 或 TACACS+ 的网络设备。
- 为满足大型网络环境的需求而设计，支持冗余服务器、远程数据库、数据库复制以及备份服务。
- 思科安全 ACS 快捷版可为中小型企业 (SMB) 提供功能强大而成本经济的解决方案。
- 思科安全 ACS 视图版增强了报告、监控及故障排除功能，满足最高级别的可见性、控制及合规性要求。

有关详情，请访问：
http://www.cisco.com/go/acs



目录

退出

思科企业策略管理器 (EPM)

概述

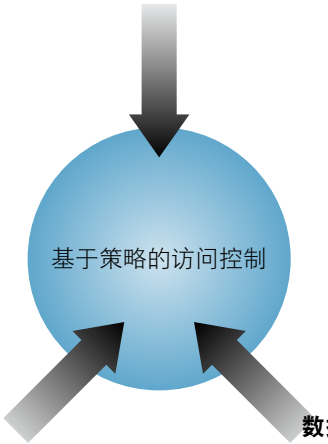
- 思科® 企业策略管理器 (EPM) 是一款市场领先、基于策略的授权解决方案，提供细致而差异化的访问控制，保护企业的应用与数据安全。
- 思科企业策略管理器 (EPM) 可将策略决策服务从现有的应用、协作服务和网络基础设施中分离出来。
- 思科企业策略管理器 (EPM) 通过提取公司的业务逻辑，实现从各单独的应用来进行公司的策略决策。这种将策略与应用逻辑松散结合的方式，可以更轻松（也更快速）地应对不断变化的法规及业务需求。
- 思科企业策略管理器是思科服务导向网络架构 (SONA) 战略的组件，网络成为服务导向架构 (SOA)、Web 2.0、协作、统一通信和企业应用的策略服务提供商。

好处

- 对授权策略进行一致的管理与实施（“configure not code”）：
  - 集中化、委托式管理，非开发人员也可使用
  - 在本地资源及远程托管资源上采用一致的应用方式
- 集中审计与实时补救：
  - 策略假设分析
  - “访问者及访问内容”等综合信息
- 符合标准的企业级产品，随买即可与客户现有基础设施实现集成
- 可根据企业规模灵活扩展，适用于从单一应用到不同的业务线 (LoB) 及跨国企业

有关详情，请访问：
http://www.cisco.com/go/epm

可访问性
- Joe（HR 管理员）是否可从“不可信”网络访问 HR 应用?



职能
- Joe 是否可以查看员工资料?
- 他是否可以调整薪资（若可以，有何额度/批准程序）？

数据
- Joe 可以看到员工资料的哪些内容?
- 他是否有权查看“EMEA”员工的地址，是否可以看到所有副总裁及其直接下属的个人数据?

目录

退出

交换机安全

首页

Cisco Catalyst 6500 系列安全服务模块

概述

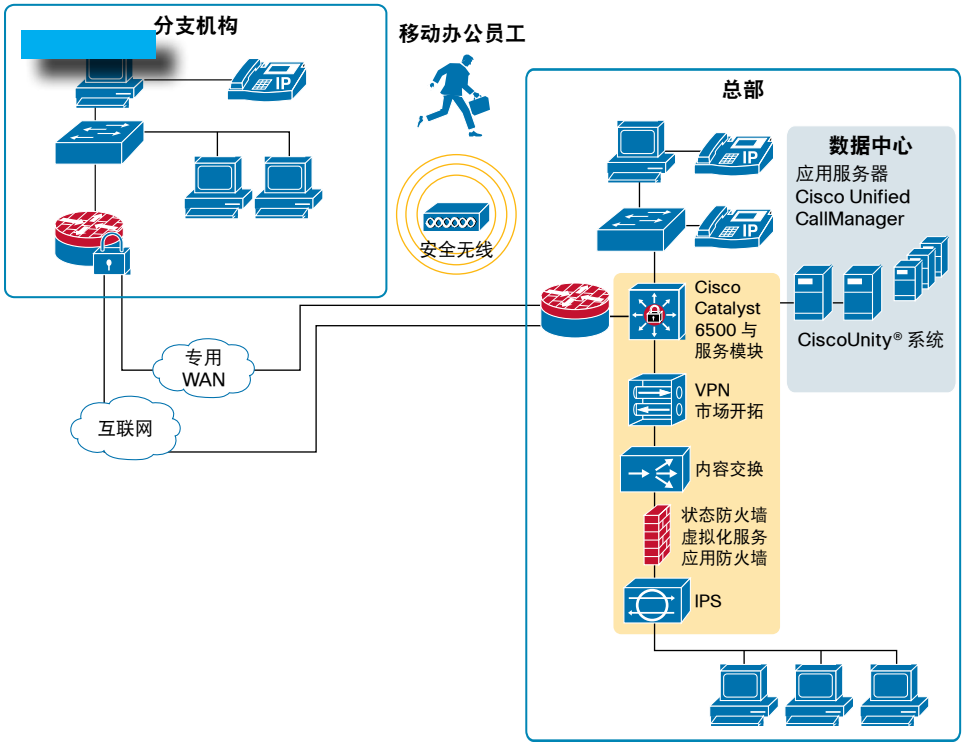
- Cisco® Catalyst® 6500 系列交换机配备一整套高级安全模块，可提供集成化网络安全保障， 其中包括防火墙、入侵防御系统 (IPS)、IP 安全 (IPsec) VPN、安全套接字层 (SSL) 加速、分布式拒绝服务 (DDoS) 以及内容交换模块等。
- 这些安全模块为网络连接性、各类服务与应用提供可用性高、适应性强且支持扩展的集成安全性能。

好处

- 可在保护现有 Cisco Catalyst 6500 系列投资的同时提高安全性能
- 紧密集成的基础设施安全解决方案
- 业界性能最佳的安全解决方案，采用单一 Cisco Catalyst 6500 系列交换机提供多千兆位性能
- 提供应用级基础设施可见性
- 与新兴科技（如应用网络服务）开展合作的重要平台

有关详情，请访问：
http://www.cisco.com/go/switchsecurity

Cisco Catalyst 6500 系列安全服务模块在网络中的应用。



目录

退出

交换机安全

首页

Cisco TrustSec

概述

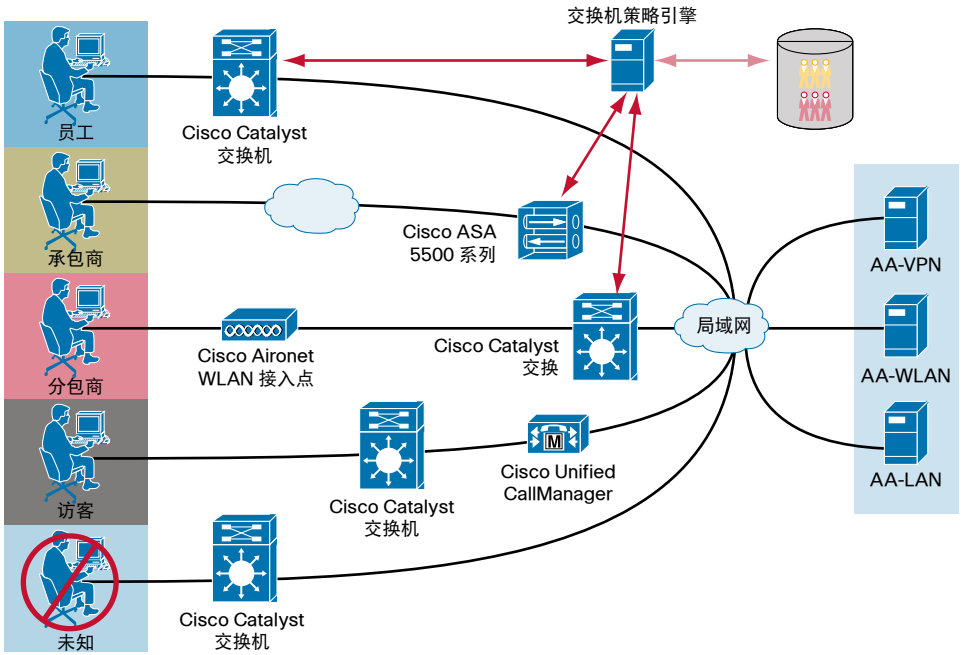
- Cisco® TrustSec 提供安全园区访问控制，可根据用户在企业中的角色进行访问控制，从而保护客户的数据及资源。采用独立运作方式，与用户接入网络的时间、地点和方式无关。
- Cisco TrustSec 可采用集成化策略框架。TrustSec 可帮助客户将多种访问策略整合成集成化策略框架，保证一致性和可扩展性。TrustSec 还可作为园区网络基础设施与后端策略目录（例如活动目录）之间的代理。
- Cisco TrustSec 提供广泛的完整性和机密性保护。TrustSec 可在交换机端口间提供交换机级别的逐跳加密，从而保护敏感数据，挫败中间人攻击。

好处

- 提供基于角色的身份验证，有效控制对重要应用与资源的访问
- 将各类角色、服务器及访问定义融合成集中式策略框架，并简化基于身份的策略管理
- 防止数据丢失，满足法规要求
- 与思科基于身份的网络服务 (IBNS) 配合使用，提供灵活的身份验证和策略控制
- 提供可扩展的交换机安全服务
- 优化策略管理与实施，创造新的业务机会，提升安全性能，降低 IT 总成本，同时满足合规性要求

有关详情，请访问：
http://www.cisco.com/go/trustsec

Cisco TrustSec 在网络中的应用。



目录

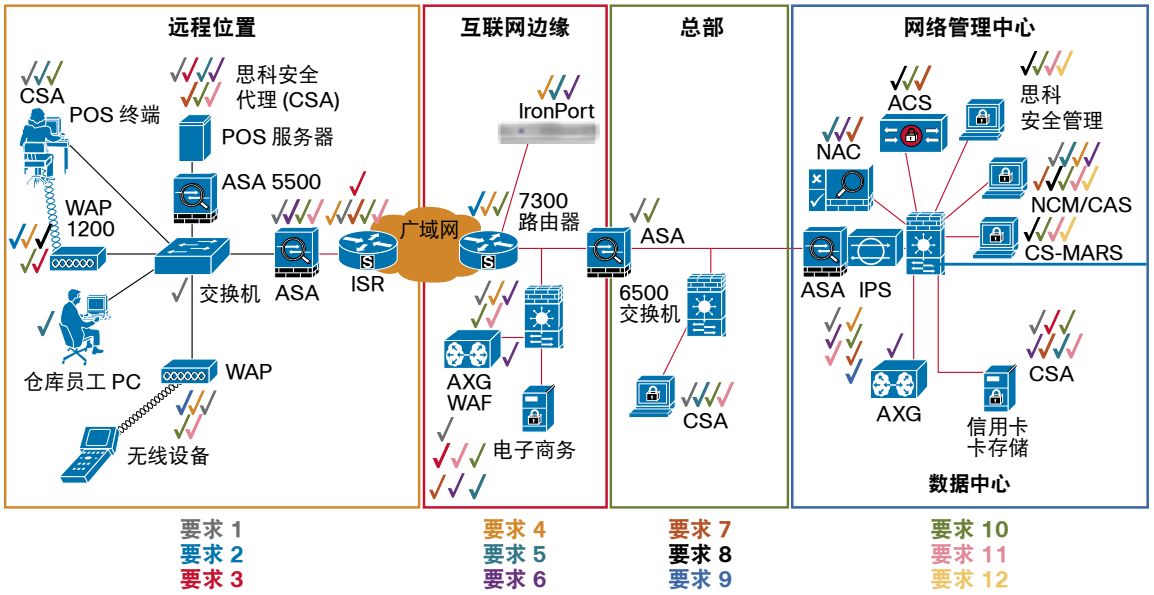
退出

解决方案

合规性

概述

- 支付卡行业 (PCI) 标准是全球性的行业标准，用于在处理、传输或存储客户信用卡信息期间保护客户信用卡信息。
- Cisco® PCI 验证架构是经 PCI 合格安全评估机构 (QSA) 审计的一整套架构，满足多项 PCI 要求。
- 思科 PCI 解决方案包括下列思科产品及服务：
  - Cisco ASA 5500 系列自适应安全设备，配备防火墙、VPN 以及 IPS
  - 思科集成服务路由器及防火墙、VPN 和 IPS 上的 Cisco IOS® 软件
  - 思科无线控制服务器 (WCS) 的统一无线网络、无线局域网控制器以及 Aironet® 1100 和 1200 系列无线接入点
  - 思科安全代理
  - 思科安全监控、分析和响应系统（思科安全 MARS）
  - 思科安全管理器
  - CiscoWorks 网络合规管理器
  - 思科网络准入控制 (NAC) 设备
  - Cisco IronPort® 邮件安全
  - Cisco ACE WAF
  - Cisco IPS 4200 系列入侵防御系统设备
  - Cisco Catalyst® 6500 系列防火墙服务模块 (FWSM) 与入侵检测服务模块 (IDSM-2)
  - 思科安全访问控制系统 (ACS)
  - 提供专业服务，满足 PCI 遵从性要求，并保持遵从状态
- 思科及思科安全专业化认证合作伙伴提供的思科 PCI 服务包括：
  - 思科 PCI 差距分析服务
  - 思科 PCI 补救服务
  - 思科 PCI 远程监控和管理服务
  - 思科 PCI 定期差距分析服务



目录

退出

合规性
（续）

好处

- 通过建立切实可行的 PCI 验证架构，降低网络复杂性与开支，减少处罚风险
- 帮助企业逐步满足 PCI 遵从性要求
- 展示客户如何充分利用现有的思科投资
- 提供方便用户及审计员使用的 PCI 报告，可减少审计时间与费用
- 提供集成化端到端解决方案，价值高于单一产品

有关详情，请访问：

http://www.cisco.com/go/compliance

思科虚拟办公室

概述

远程办日益广泛，这归因于全球化、燃油和能源价格上涨、“绿色”计划实施、以及用于业务通信的协作应用不断增加。思科® 虚拟办公室：

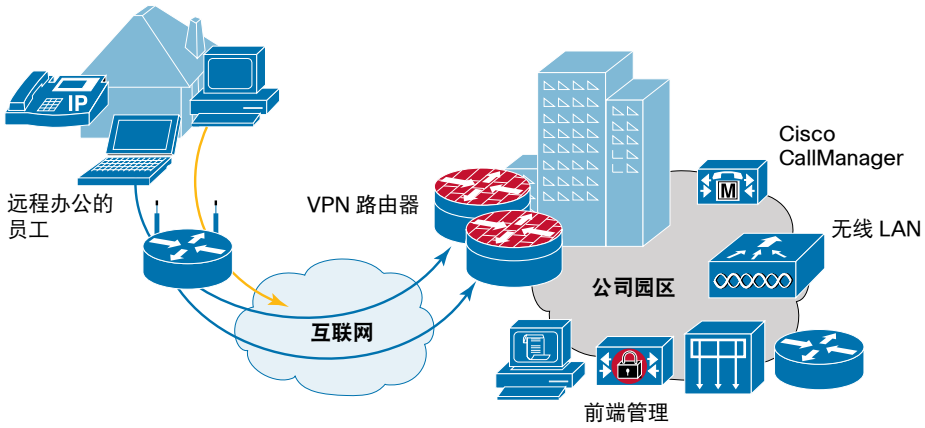
- 使企业可以在集中管理的环境中提供数据、语音、视频和无线移动服务，从而将工作空间扩展到远程工作者。
- 通过集成化服务路由器平台提供专用 VPN、防火墙、IPS 和内容安全功能，满足远程工作者的安全要求。
- 通过提供与传统公司环境相同的 IT 服务，让远程工作者享受无缝办公体验。

思科虚拟办公室 (CVO) 架构是家庭办公室、小型分支机构、呼叫中心、移动业务伙伴及合同制员工的理想之选。

面向家庭办公用户的思科虚拟办公室部署。

该网络可实现：

- 办公室级别的数据、语音和视频服务
- 可扩展至远程用户的集成化安全性能
- 可扩展的低成本 VPN 架构



目录

退出

思科虚拟办公室
（续）

对员工的好处

- 工作安排更加灵活，工作与生活更加平衡
- 减少成本与通勤时间
- 提高协作工作的可靠性和访问，可提升工作效率
- 易于使用和安装

对公司的好处

- 实施一致的安全策略，进一步降低风险
- 易于管理及调整 IT 规模
- 保持操作连续性和业务灵活性
- 节省物业、能源与运营等相关成本
- 可吸引与保留人才

有关详情，请访问：
http://www.cisco.com/go/cvo

目录

退出

虚拟专用网 (VPN)

首页

站点到站点 VPN

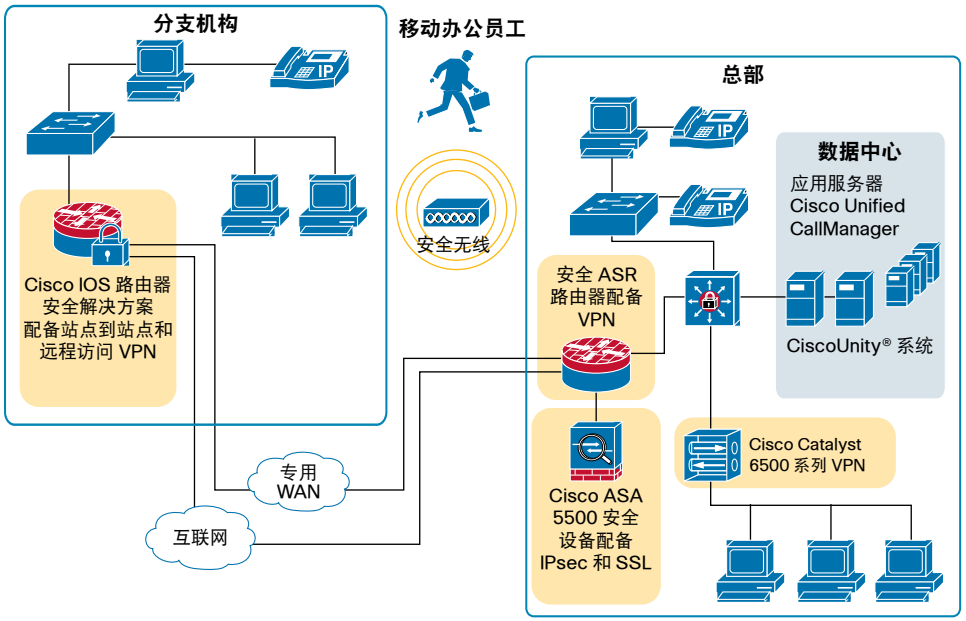
概述

VPN 可实现快速、可靠及安全的连接部署，适用于远程办公室、业务合作伙伴地点以及其他分支站点。这些地点之间的数据、语音及视频通信在经过不可信网络时仍保持机密状态。思科拥有各种 VPN 解决方案，可提供经济、高效、易于管理的安全连接。

思科提供多种 VPN 技术，包括 IPsec VPN、动态多点 VPN (DMVPN) 以及分组加密传输 VPN (GET VPN)，并将其集成至单一平台，减少了设备成本和管理复杂性。总体而言，这些解决方案属于业界最全面、扩展性最高的 VPN 产品组合。

- 思科® VPN 解决方案具备集成的威胁防护 VPN 功能，可防止恶意软件和黑客入侵，无需另外部署安全设备，不会增加成本与复杂性。
- 思科 VPN 解决方案包括
  - 思科路由器：思科最先进的站点到站点 VPN 解决方案，集成远程访问、防火墙、入侵防御系统 (IPS) 与内容安全服务
  - Cisco ASA 5500 系列：思科最先进的远程访问 VPN 解决方案，集成站点到站点 VPN、远程访问 VPN、防火墙、IPS 与内容安全服务
  - Cisco Catalyst® 6500 系列：思科扩展性最强的 VPN 平台，集成防火墙和 IPS 服务

思科站点到站点 VPN 在网络中的应用。



目录

退出

虚拟专用网 (VPN)

站点到站点 VPN
（续）

好处

- 站点到站点 VPN 可实现不同办公地点的安全连接，通过互联网降低成本、增加灵活性。
- 采用单一平台支持多 VPN 技术，可降低成本和复杂性，同时可根据部署环境定制 VPN 服务。
- 具有完全网络感知的 VPN 可向任何地点提供任何应用，包括语音和视频，且保证高度的完整性。
- 集成化威胁保护 VPN 服务可防止网络威胁，无需另外增加安全设备。

有关详情，请访问：
http://www.cisco.com/go/vpn

目录

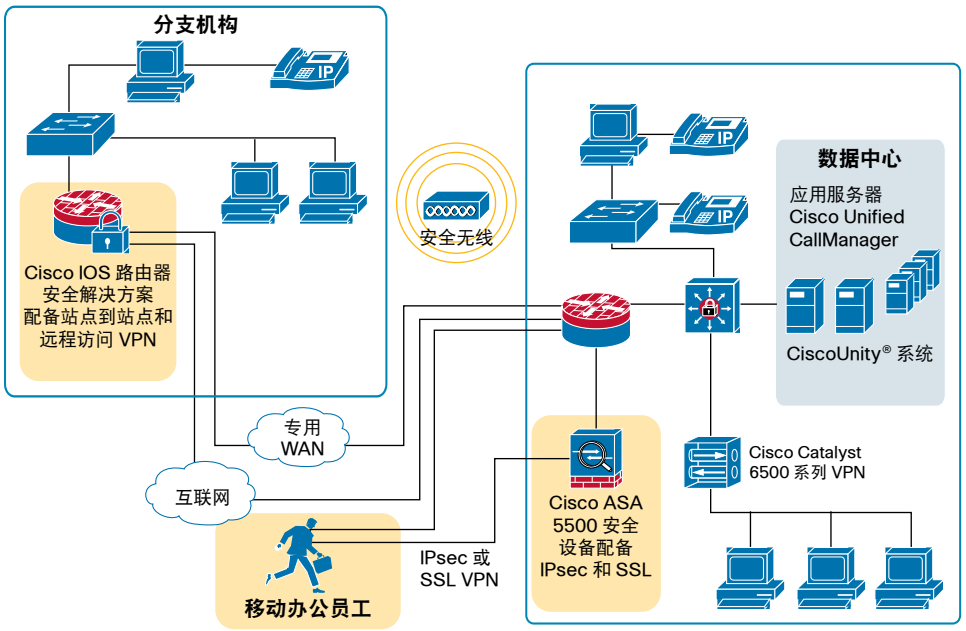
虚拟专用网 (VPN)

首页

远程访问 VPN

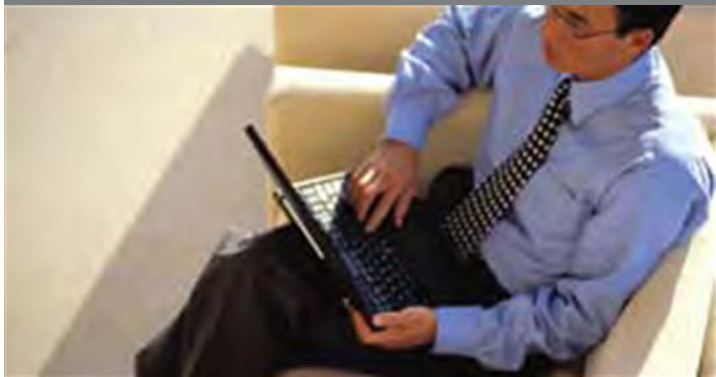
概述

- 借助远程访问 VPN，可快速、可靠、安全地从几乎任何位置随时使用任何设备连接到公司网络。无论是远程工作者、员工、承包商还是业务合作伙伴，都可以根据用户角色对公司网络进行安全的远程访问。思科提供各种 VPN 解决方案，包括 IP 安全 (IPsec) 与安全套接字层 (SSL) VPN，可实现经济高效且易于管理的远程连接。
- Cisco® VPN 集成在单个平台上，思科 VPN 解决方案包括：Cisco ASA 5500 系列：思科最先进的远程访问 VPN 解决方案，可将并发用户会话从 10 扩展到 10000 个，而且集成站点到站点 VPN、防火墙、入侵防御系统 (IPS) 和内容安全服务
- 思科路由器：思科最先进的站点至站点 VPN 解决方案，集成远程访问、防火墙与 IPS 服务
- 思科 VPN 解决方案包括：
  - Cisco ASA 5500 系列：思科最先进的远程访问 VPN 解决方案，可将并发用户会话从 10 扩展到 10000 个，而且集成站点到站点 VPN、防火墙、入侵防御系统 (IPS) 和内容安全服务
  - 思科路由器：思科最先进的站点至站点 VPN 解决方案，集成远程访问、防火墙与 IPS 服务
  - Cisco Catalyst 6500 系列：思科扩展性最强的 VPN 平台，集成防火墙和 IPS 服务



目录

退出



虚拟专用网 (VPN)

远程访问 VPN
（续）

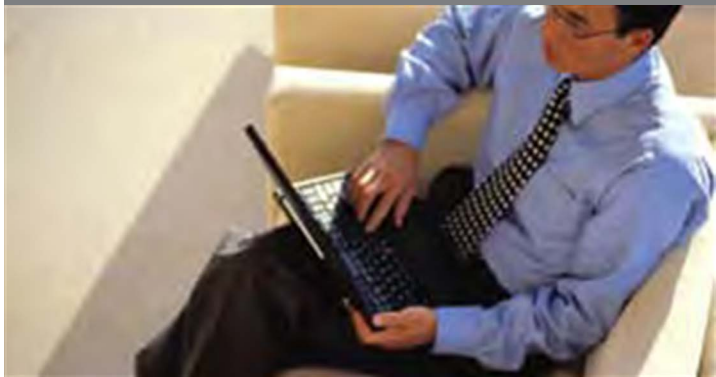
好处

- 远程访问 VPN 使远程工作者可使用任何设备随时随地安全访问网络，提高了工作效率；可使用设备包括 PDA、智能手机、公共服务网点、个人笔记本电脑以及共享计算机。访问可根据用户角色进行定制，如在加班者、全职员工、远程工作者、合同制员工或业务合作伙伴。
- 远程访问 VPN 通过单一平台同时支持 IPsec（远程访问与站点到站点）及 SSL VPN 连接，既降低了成本、复杂性和管理费用，又可根据部署环境定制 VPN 服务。
- 远程访问 VPN 支持 IPsec 与无客户端 SSL VPN。
- 具有完全网络感知的 VPN 可向任何地点提供任何应用，包括语音和视频，且保证高度的完整性。
- 集成化威胁防护服务可防止病毒、间谍软件与黑客跨过 VPN 连接，无需另外增加安全设备。
- 无客户端 SSL VPN 可使用标准 Web 浏览器，从任何联网地点实现远程访问连接，从而简化了网络管理。

有关详情，请访问：
http://www.cisco.com/go/sslvpn

目录

退出



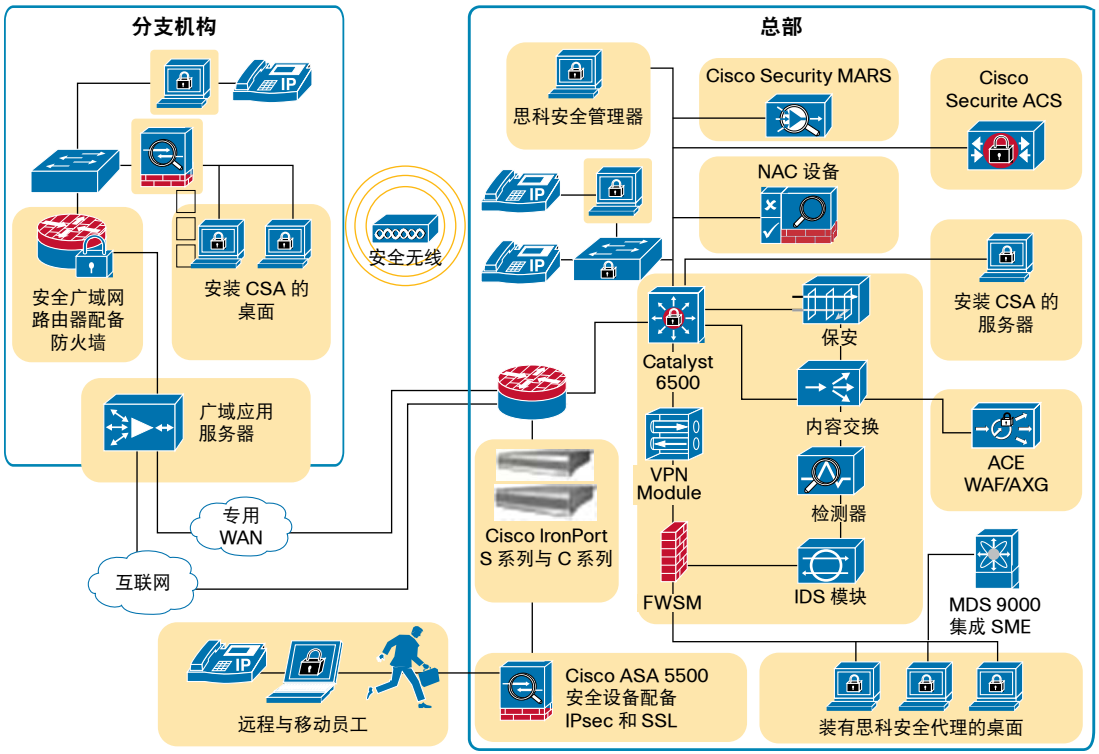
合而为一

首页

思科® 自防御网络提供业界最全面的端到端网络安全方法。思科拥有世界一流的解决方案，不仅具备同类最佳的功能和特性，还可提供无可比拟的安全保护，主要实现方式包括：

1. 集成：关键安全功能已经融入思科整个应用设备与网络设备系列，同时也融入我们关键的业务应用与服务（如统一通信和数据中心）当中。
2. 协作：通过在安全设备与网络设备之间、不同的安全设备与解决方案之间进行前所未有的协作，额外增加了一层安全性。
3. 适应性：思科解决方案可以识别网络任何位置的安全事件，并在全网络共享该信息，从而可根据实时的威胁与事件，动态调整网络的总体安全配置文件。

这种集成化、协作性与适应性安全方法可提供全面、深入的防御，最大程度地降低风险，减少总体拥有成本，是保护您网络环境安全的理想选择。



目录

退出