

# 防范安全威胁，简化服务提供流程

客户案例研究



## 执行摘要

**组织:** Gobierno de Castilla-La Mancha (卡斯蒂利亚-拉曼查自治区政府)

**行业:** 政府

**地区:** 西班牙

**员工:** 63,000 名

### 挑战

- 简化政府的公共服务提供流程
- 识别用户的浏览习惯以便分配相应的安全策略
- 通过易于部署的邮件安全解决方案更新并简化邮件管理

### 解决方案

- 思科网络安全设备
- 思科邮件安全设备
- Cisco ASA 5585-SSP-60 自适应安全设备

### 成果

- 显著降低外部互联网访问恶意软件威胁，同时改善用户体验
- 实现稳定的邮件安全性，并大大提高性能
- 提供易于部署和管理的解决方案，使 IT 员工可以有时间处理其他活动

Gobierno de Castilla-La Mancha 使用网络安全设备和邮件安全设备为互联网访问和邮件提供安全保护。

## 挑战

Gobierno de Castilla-La Mancha 是西班牙卡斯蒂利亚-拉曼查自治区地方政府，为居住地极为分散的 200 多万名居民提供医疗、教育和行政服务。该地区政府雇用将近 20,000 名医疗保健工作者，18,000 名教育从业者，12,000 名远程工作人员，以及 12,000 名行政人员。政府还负责管理本地区的农业和经济事务。

面对西班牙最大自治区内如此众多的员工，只有四名 IT 专业员工负责实施和管理 IT 网络以及安全。在资源有限的情况下，IT 团队必须简化操作才能为本地区的居民和企业安全提供服务。

“我们为教师、医疗保健工作者以及政府雇员提供互联网服务。每一类人员都需要在工作中访问不同的网站，” Gobierno de Castilla-La Mancha 社区理事会信息技术协调人 Pedro Jesus Rodriguez Gonzalez 说。“我们所需的解决方案应该能够管理不同的身份，管理不同人员访问网站的 URL，并在需要时快速解析被阻止的地址。”

在用户访问和身份纷乱复杂的情况下，如何保证稳健的网络安全性是一个关键问题。组织需要一种更为简化的方式来控制不同的用户配置文件，并确保在核心网络得到保护的情况下众多用户都能访问他们所需的资源。他们还需要在不增加更多员工的情况下能够集中管理规模日益扩大的网络。

此外，为满足地区的发展需求，IT 团队需要找到有效的方式为具有 100,000 名用户的邮件系统提供安全保护并且每天处理多达 500,000 条消息，保护网络不受入站和出站邮件威胁的侵害。

“以前我们必须收集多方线索才能形成报告。而使用 Cisco WSA，当用户报告问题时，我们可以十分容易地了解问题的根本原因，从而有效解决问题。”

---

**Pedro Jesus Rodriguez Gonzalez**  
Gobierno de Castilla-La Mancha  
信息技术社区委员会协调人

## 解决方案

卡斯帝里亚-拉曼查政府的 IT 团队需要一种既可满足身份和访问策略需求，又具备十分稳定的网络安全性的解决方案。在研究不同的市场可选方案之后，IT 团队选用了思科® 网络安全设备 (WSA)、思科邮件安全设备 (ESA) 以及 ASA 5585 自适应安全设备来帮助帮助他们满足组织的需求。同时，思科身份服务引擎 (ISE) 和 TrustSec® 为无线设备访问网络提供支持。

借助 Cisco WSA，政府现在具备了更强的威胁防范能力，更高级的恶意软件保护功能，并实现应用可见性和可控性功能。

“在实施思科解决方案之前，我们需要耗费大量时间管理众多黑名单和白名单，而恶意软件防护和 URL 管理工作更是极为耗时。由于分类错误的比率极高，导致用户使用不便，而可用率也十分低下，” Rodriguez Gonzalez 说。

此外，IT 团队还需要简单而又具有洞察力的报告功能。“以前我们必须收集多方线索才能形成报告，” Rodriguez Gonzalez 说。“而使用 Cisco WSA，当用户报告问题时，我们可以十分容易地了解问题的根本原因，从而有效解决问题。”

WSA 解决方案还使卡斯帝里亚-拉曼查政府能够完全控制最终用户访问互联网的方式。通过对数百个应用以及 150,000 多个微型应用进行识别，WSA 帮助 IT 员工建立了不同的策略用以满足医疗、教育和政府职员的不同需要。可以根据部门和用户的需求允许或阻止聊天、消息传送、视频和音频等具体功能，而无需阻止整个网站。

卡斯帝里亚-拉曼查政府还借助思科邮件安全设备 (ESA) 实现高级威胁保护以及垃圾邮件过滤功能，并使得各项策略更易于推行。

“面对每天 50 多万封邮件，数量不断增长的垃圾邮件始终是令人头疼的难题，” Rodriguez Gonzalez 说。

在 ASA 5585 自适应安全设备的帮助下，卡斯帝里亚-拉曼查团队可以对进出各个地区服务网络的不同部分以及具有自建网站的众多企业网络的访问行为进行控制，根据情况允许或拒绝这些访问。

此外，Rodriguez 还提到上班族用户主要使用移动设备，如笔记本电脑，而其他用户则使用台式机或工作站。卡斯帝里亚-拉曼查政府通过使用身份服务引擎监控执行访问的用户、所访问的网络范围以及使用的设备种类，同时配合无线控制器保护网络安全，从而完美解决这两类用户的需求。

## 成果

新的解决方案带来了立竿见影的效果。通过使用内容安全管理设备，IT 团队现在可以采用更加集中的方式查看由 WSA 提供保护的整个网络，并实现按需报告功能。实时跟踪网络流量的功能帮助团队管理可能出现的威胁，并在需求发生变化时做出调整。

通过加入更精细化的报告功能，卡斯帝里亚-拉曼查政府 IT 团队可以安全地生成特定报告，包括最常访问的网站、带宽使用情况以及阻止的病毒和恶意软件等信息。

团队可以根据特定网站的分类方式生成报告，从而了解用户最常访问的网站类别，例如政府和法律部门网络或社交网络。

WSA 使用户的在线体验更好更稳定，性能、吞吐量和冗余度均得到改善。现在，用户只需要在开始访问时提供一次凭证即可，而团队还计划在未来实现单点登录功能。



今后，该团队也准备借助 ISE 和 TrustSec 来集成有线网络，以便验证、授权和控制用户的 VPN 使用。这将使卡斯蒂里亚-拉曼查团队实现更好的安全性控制。

## 更多详情

有关所使用的思科安全产品的更多信息，请访问：

- <http://www.cisco.com/go/wsa>
- <http://www.cisco.com/go/esa>
- <http://www.cisco.com/go/asa>
- <http://www.cisco.com/go/ise>
- <http://www.cisco.com/go/trustsec>
- <http://www.cisco.com/go/sma>

### 产品列表

#### 安全

- 思科网络安全设备
- 思科邮件安全设备
- Cisco ASA 5585-SSP-60 自适应安全设备
- 思科内容安全管理设备
- 思科身份服务引擎
- Cisco TrustSec

#### 数据中心

- 思科统一计算系统™
- Cisco Vblock 系统
- 思科 6248 和 6124 交换矩阵互联

#### 路由器和交换机

- 思科 7204 路由器
- Cisco Nexus 3500 系列交换机
- Cisco Catalyst 6509 交换机



美洲总部  
Cisco Systems, Inc.  
加州圣荷西

亚太总部  
Cisco Systems (USA) Pte. Ltd.  
新加坡

欧洲总部  
Cisco Systems International BV Amsterdam,  
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 上列出了各办事处的地址、电话和传真。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问以下 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标均为其各自所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作关系。(1110R)