Protecting Against Security Threats, Streamlining Service Delivery

Customer Case Study

EXECUTIVE SUMMARY

Organization: Gobierno de Castilla-La Mancha (Government of Castilla-La Mancha)
Industry: Government
Location: Spain
Employees: 63,000

Challenge

- Streamline delivery of regional government's public services
- Identify users' navigation habits to assign appropriate security policies
- Update, simplify email management with easy-to-deploy email security solution

Solution

- Cisco Web Security Appliance
- Cisco Email Security Appliance
- Cisco ASA 5585-SSP-60 Adaptive Security Appliance

Results

- Significantly reduced external Internet access malware threats, improving user experience
- Stabilized email security, dramatically improving performance
- Provided easy-to-deploy and manage solutions, freeing up IT staff time to handle other initiatives

Gobierno de Castilla-La Mancha secures Internet access, email with Web Security Appliance and Email Security Appliance.

Challenge

The Gobierno de Castilla-La Mancha, the Regional Government of Castilla-La Mancha in Spain, provides health, education, and administration services for a widely dispersed population of more than two million residents. The regional government employs approximately 20,000 healthcare workers, 18,000 educators, 12,000 remote access teleworkers, and 12,000 administrators. The government also is responsible for managing the agricultural and economic needs of the region.

A staff of just four IT professionals is responsible for implementing and managing the IT network and security for this wide range of employees across Spain's largest area. With limited resources, the IT team must rely on streamlining their operations to securely deliver services to the region's residents and businesses.

"We provide Internet services for teachers, healthcare workers, as well as government employees. Each group has websites they visit as part of their jobs," says Pedro Jesus Rodriguez Gonzalez, coordinator, Information Technology, Community Board, Gobierno de Castilla-La Mancha. "We needed a solution that could manage the different identities, manage the URLs of the websites they were visiting, and quickly resolve blocked addresses, if necessary."

Maintaining strong network security in the face of the different user access and identities was a concern. The organization needed a more simple way to control the different user profiles and to make sure users could get to the resources they needed while still protecting the core network. They also needed to be able to centrally manage their significantly expanded network without adding more staff.

Additionally, to address the needs of the growing region, the IT team also needed a way to secure its email system of 100,000 users and to handle 500,000 messages per day, protecting the network from inbound and outbound email threats.

"Previously, we had to piece together reports. With the Cisco WSA, when a user reports a problem, it's easy to see what they are talking about and address the issue."

Pedro Jesus Rodriguez Gonzalez
Coordinator, Information Technology Community Board
Gobierno de Castilla-La Mancha

Solution

Castilla-La Mancha's IT team sought a solution that could meet identity and access policy requirements, along with additional robust web security. After researching different market options, the IT team selected the Cisco® Web Security Appliance (WSA), Cisco Email Security Appliance (ESA), and ASA 5585 Adaptive Security Appliance to help them address the needs of the organization. Cisco Identity Services Engine (ISE) and TrustSec® support the use of wireless devices accessing the network.

With the Cisco WSA, the government now has better threat defense, advanced malware protection, and application visibility and control.

"Before the Cisco solution – particularly in regards to our malware and URL management – we had to spend a lot of time managing black lists and white lists. There was a huge misclassification rate, which led to challenges for users and a low availability rate," says Rodriguez Gonzalez.

In addition, the IT group needed easy, insight-filled reporting. "Previously, we had to piece together reports," says Rodriguez Gonzalez. "With the Cisco WSA, when a user reports a problem, it's easy to see what they are talking about and address the issue."

The WSA also gives Castilla-La Mancha complete control over how end users access the Internet. By identifying hundreds of applications and more than 150,000 micro-applications, the WSA has helped the IT staff create policies that match the different needs of healthcare, education, and government employees. Specific features such as chat, messaging, video, and audio can be allowed or blocked, according to the requirements of various departments and users – without the need to block entire websites.

Castilla-La Mancha also relies on the Cisco Email Security Appliance (ESA) to provide advanced threat protection, block spam, and deliver easy enforcement of policies.

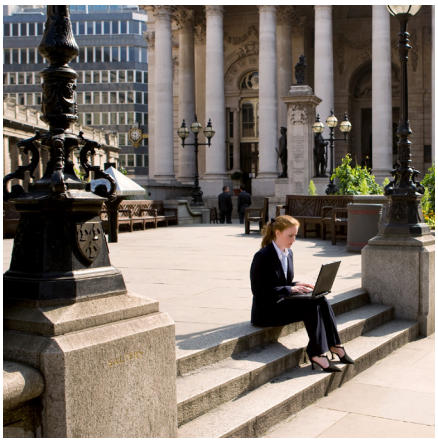
"With more than a half-million emails per day, rapidly rising spam volumes are a continual challenge," says Rodriguez Gonzalez.

The ASA 5585 Adaptive Security Appliance enables the Castilla-La Mancha team to allow or deny access to and from the different parts of their distinct regional services and corporate network, each with their own website.

He also notes that the work population includes users who rely on mobile devices such as laptops, while others use desktops or workstations. Castilla-La Mancha can address the wireless needs of both by protecting the network using the Identity Services Engine to monitor who has access, to what part of the network and using what device, in concert with the Wireless Controller.

Results

The results of the new solutions have been seen almost immediately. The IT team now has a more centralized view and on-demand reporting capabilities of their entire network of WSAs through the Content Security Management Appliance. The ability to track web traffic in real-time enables the team to manage threats as they arise and to make changes as needs change.



The addition of more granular reporting enables Castilla-La Mancha to securely create specific reports, including top visited websites, bandwidth usage, and viruses and malware that have been blocked.

The team can produce reports according to how their specific websites are categorized, to know which category is the most visited by users, such as government and law, or social networking.

WSA has provided a better, more reliable online experience for its users with improved performance, throughput, and redundancy. Users also need only to provide their credentials once; the team is looking at leveraging single sign-on in the future.

In the future, the team aims to leverage ISE and TrustSec also to integrate wired networks in order to authenticate, authorize and account for their VPN use. This will give the Castilla-La Mancha team greater security controls.

For More Information

To find out more about the Cisco Security products used, go to:

- 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

PRODUCT LIST

Security
- Cisco Web Security Appliance
- Cisco Email Security Appliance
- Cisco ASA 5585-SSP-60 Adaptive Security Appliance
- Cisco Content Security Management Appliance
- Cisco Identity Services Engine
- Cisco TrustSec

Data Center
- Cisco Unified Computing System™
- Cisco Vblock System
- Cisco 6248 and 6124 Fabric Interconnects

Routers and Switches
- Cisco 7204 Routers
- Cisco Nexus 3500 Series Switches
- Cisco Catalyst 6509 Switches

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C36-732189-00 07/14