Use Case

CISCO ISE

THE CLIENT

An independent federal authority that supports the telecommunications needs of public safety organizations across the United States.

THE NEED

Port-based authentication requiring login credentials for wired, wireless and VPN users.

THE SOLUTION

Cisco Identity Services Engine (ISE)

OVERVIEW

Based in Reston, Virginia, this client provides specialized communications services for emergency services at local, state, tribal and federal levels. An outgrowth of laws originating with the 9/11 Commission, this organization was established to create a nation-wide network and provide wireless services to public safety agencies across the country.

With members from a wide range of defense agencies, this client's mission directly affects national security and public safety—including telecommunications infrastructure. With a wealth of highly sensitive data at its disposal, this client needed a reliable, high-quality access control solution to protect its network from unauthorized users and to provide authorized users with appropriate access levels and security measures on their devices.

THE SOLUTION

Having previously worked with Force 3 to design and deploy its existing network, the client once again reached out, this time for assistance in deploying a wireless solution. Recognizing the additional need for improved access control, Force 3 recommended Cisco ISE, which promised the most cost-effective, seamless integration with its existing Cisco network environment.

Together, multiple engineers spent several weeks onsite with the client to assess, plan, design, configure and, ultimately, implement Cisco ISE across the network—including wired, wireless and VPN environments. That process included (but was not limited to):

- Making environment-wide changes
- Configuring network access devices
- Creating certificate templates
- Performing endpoint configurations
- Trouble-shooting specific devices
- Ensuring scalability for the necessary number of users and devices
- Testing for failure resistance, redundancy and availability
- Ensuring the appropriate client and software choices
- Security posture assessment and profiling to ensure any devices connecting to the network had up-to-date software/anti-virus and appropriate permissions

Because organization-wide adoption is critical to a solution's success, Force 3 also collaborated with the client to establish the proper training and resources to ensure the organization continues using and benefiting from Cisco ISE. That includes providing ongoing support and education to help the client use this solution to its fullest capabilities.

COMPANY HIGHLIGHTS

- 27 years serving federal clients
- CRN Solution Provider 500 (since 2010)
- CRN Tech Elite 250 (since 2011)
- Large Federal contracts portfolio
- Highest partnership levels with leading manufacturers
- ISO 9001 Certified
- Regional Technology Enablement Centers
- First Federal partner to pursue Partner Support Service program for Public Sector
- A state-of-the-art Managed Services Command Center

THE OUTCOME

As expected, ISE offered a seamless, high-value integration with the client's Cisco network technology. Through Cisco ISE, Force 3 provided multiple functionalities for device authentication, network administrators and certificate authentication, all from one platform and with centralized management capabilities (i.e., a single pane of glass). Further still, through ongoing support and collaboration, the client's IT team can continue maximizing its use and adoption of Cisco ISE and all the benefits it offers.

Ultimately, the client can move forward with confidence, knowing that its network—and all the sensitive, mission-critical data it holds—is secured with a best-in-class access control solution.

Cisco Gold Partner | Cisco Master Security Partner | Cisco Master Collaboration Partner | Cisco Master Cloud Builder Partner | Cisco Lifecycle Advisor Partner