Red River Case Study

NATIONAL SCIENCE FOUNDATION ENHANCES SECURITY AND CONTROL WITH RED RIVER AND CISCO® IDENTITY SERVICES ENGINE

KEY BENEFITS

- Enabled Secure Enterprise Mobility
- Maximized Network Security and Control
- Centralized and Unified Network Access Policy Management
- Empowered Extreme Flexibility and Scalability
- Ensured Compliance
- Simplified Support with Ongoing Managed Services from U.S.-Based Network Operations Center

TECHNOLOGY

- Cisco Identity Services Engine (ISE)
- Cisco AnyConnect Secure Mobility Client
- Cisco 802.1x Port-Based Authentication
- SSL VPN & WEB VPN
- PKI & Common Access Cards

CHALLENGE

While embracing mobility and actively developing a Bring Your Own Device (BYOD) strategy, the National Science Foundation (NSF) wanted to minimize security risks, increase visibility and ensure control over the computers and mobile devices connecting to their network, whether on-site at their headquarters or from remote locations. They needed a simplified Identity-Based Access and Management tool to automate and enforce secure access to NSF network resources, regardless of where users were connecting or which type of device they were using. With a Federally-regulated mandate to use 8021.x in conjunction with PKI, security and compliance were top priorities. Moreover, NSF planned to consolidate their wired and wireless networks and expand their wireless reach in the near future. So, any new network and identity access and management solution needed to scale easily, be highly available and allow NSF to enforce security policies consistently over VPN, wired and wireless networks. NSF also hoped to leverage their existing Cisco Secure Access Control System (ACS) to minimize costs and disruption.

SOLUTION

Red River helped the NSF implement a customized, highly secure and scalable Cisco Identity Services Engine (ISE) solution that works seamlessly with their existing network, is easy to support and provides comprehensive visibility and control for network authentication, regardless of user device or location.

A Proven Approach with Expert Support

Red River worked closely with NSF to understand their key challenges and constraints, current infrastructure, the types of clients that would be connecting to the network as well as the security and management policies NSF wanted to enforce. As NSF was already using Cisco ACS, Red River recommended transitioning to Cisco Identity Services Engine (ISE) in order to utilize their current Cisco infrastructure. NSF end users rely on both Windows-based and Apple devices, so Red River also kept this in mind as they customized the solution for NSF.

To demonstrate the expansive capabilities, high availability and reliability of Cisco ISE and integrate ISE with minimal disruption, Red River designed a Pilot program for NSF with use cases based on NSF user policies and limited to authentication, authorization and profiling. Red River then physically installed and configured Cisco ISE appliances, network access devices (switches), workstations, wired and VPN connections. Red River also profiled and authenticated 200-400 remote users before allowing network access. .

At the end of the Pilot, and after policy validation, Red River transitioned NSF's ISE implementation to Monitor Mode to validate that all devices were authenticating correctly, either with 802.1x or MAC Authentication Bypass (MAB). Once confident that endpoints were configured correctly, Red River transitioned ISE to Authenticated Mode for wired and VPN connections. In this mode, a pre-authentication ACL was applied to the switch port, allowing a very limited amount of network access prior to authentication, with

Red River®

PARTNERS

ABOUT NATIONAL SCIENCE FOUNDATION

The National Science Foundation (NSF) is an independent federal agency created by Congress in 1950 to promote the progress of science; advance national health, prosperity and welfare; and to secure national defense. NSF is the only federal agency whose mission includes support for all fields of fundamental science and engineering, except for medical sciences. The agency is tasked with keeping the United States at the leading edge of discovery in areas from astronomy to geology to zoology. Learn more at www.nsf.gov.

ABOUT RED RIVER

Red River is a technology integrator committed to helping customers optimize business processes and maximize the value of technology investments. Widely regarded for our special focus on the U.S. government, Red River has developed a remarkable reputation for delivering technology solutions and services to military and civilian agencies and the companies that serve them. Our core values of hard work and honesty fuel our central mission to make IT personal.

For more information please call 800.769.3060 or visit www.redriver.com.

only DHCP, DNS and access to non-restricted resources as deemed appropriate by NSF. Authenticated endpoints and users can receive additional granular levels of access depending on NSF's authorization policy.

Technology

The Cisco Identity Services Engine (ISE) is a premier identity and access control policy platform that allows NSF to enforce compliance, enhance infrastructure security and streamline their service operations. Its unique architecture let NSF gather real-time contextual information from networks, users and devices to make proactive governance decisions by tying identity back into various network elements, including access switches, wireless controllers, VPN gateways and data center switches. For the NSF solution, Red River also utilized Cisco AnyConnect Secure Mobility Client alongside Cisco ISE to deliver context-aware, comprehensive security policy enforcement.

Partners

As a longstanding Cisco Gold Certified partner with Cisco ISE certification and one of the few Cisco partners with Master-level certifications in both Collaboration and Security in the Federal space, Red River had the expertise to recommend and transition NSF to Cisco ISE without incident. Red River also recognized that NSF was in a unique position with their existing Cisco ACS system to keep project costs low by reusing existing Cisco hardware, maximizing Cisco upgrade programs and optimizing licensing.

RESULTS

In just two weeks, NSF was up and running with Cisco ISE, actively managing 1,500 end users with the ability to easily support 5,000+ users as they expand their network. Consistent identity management and security policy enforcement across the network, regardless of access method – whether wired, wireless or VPN – is seamless. NSF administrators can easily identify devices on the network and see which users are logged into those devices, providing contextual information they can then use to make, manage and enforce policy decisions. Not only does Cisco ISE allow NSF to take advantage of additional profiling and posture feature sets, but it also simplifies ongoing management and troubleshooting.

In Summary

Using their in-depth Cisco ISE expertise, Red River transitioned NSF from Cisco ACS to Cisco ISE without disruption to day-to-day operations and customized the system to apply detailed posture assessment and enforcement capabilities for both Apple OS X and Windows clients. To ensure the compliance with stringent Federal security mandates for network access, Red River also configured SSL and Web VPN with inline posturing and integrated CAC/PKO authentication for NSF's Cisco ISE deployment. Plus, with Red River's strong Cisco partnership, expert guidance and insight, NSF had to purchase very little equipment to optimize mobility and secure network access for their users. Ongoing Managed Services are provided by Red River's New Hampshire-based Network Operations Center and NSF intends to call on Red River Professional Services as their expand their wireless network.