Case Study

Top Banking and Wealth Management Services Provider Enhances Security and Ensures Compliance with Guidance from CDCT

The client

The client is a banking and wealth management services provider listed by Forbes as one of America's 100 largest banks. Over 5,000 employees provide services in numerous banks and trusts in U.S. cities.

The challenge: Meet FDIC requirements around network access control and asset visibility, and implement a robust firewall based on compliance needs and business drivers

The client had to meet Federal Deposit Insurance Corporation (FDIC) requirements for network access control and network asset visibility. To do so, they needed assistance with designing a secure solution to authenticate, authorize, and profile network endpoints using wired access. Due to previous delays in the project, the timeline for implementation was greatly accelerated.

In addition, facing the end-of-life of its existing Juniper SRX Firewall, the client needed help with selecting and deploying a replacement to ensure it was using supported infrastructure that would not trigger a finding in an audit. They came to Cloud + Data Center Transformation (CDCT) for assistance with the full spectrum of activities related to these initiatives.

Industry:

Financial

CDCT provided:

- Cisco® Identity Services Engine (ISE)
- Cisco AnyConnect® Secure Mobility Client
- Palo Alto Networks firewall preparation & staging
- Firewall configuration, testing & deployment
- Migration to new firewall & post-deployment optimization

CDCT services:

- Consulting
- Assessments
- System architecture design & deployment
- Project management

The solution: Advanced systems for enhanced protection and more proactive security

The project provided many unexpected challenges as our team worked to meet the client's deadlines. These issues included:

Accelerated execution timeline

Provisioning certificates to the client's endpoints for network authentication

The need to refresh network access devices to support the access control solution

After providing a proof-of-concept for various use cases in a non-production environment and getting approval from the client, we implemented a Cisco Identity Services Engine (ISE) and Cisco AnyConnect Secure Mobility Client. This includes eight Cisco ISE nodes, Cisco AnyConnect deployed to 10,000 workstations, and 200 network access switches deployed with access control configuration.

To address the firewall need, our team worked with key stakeholders and decision makers throughout the company to complete an in-depth discovery process that defined the business drivers and compliance requirements that would guide the selection of the replacement. This included getting input from the CIO, network VP, managers, architects, strategists, and analysts. Next, we assessed the technology options based on the client's criteria and provided a recommendation.

Following the client's selection, our team prepped and staged the new Palo Alto Networks firewall, and configured and tested it. Then, we deployed the solution and executed a migration to the new firewall. Finally, we performed post-deployment optimization to achieve peak performance. All of this work was completed ahead of the end-of-support of the old firewall to ensure uninterrupted protection.

The benefits: 20,000+ endpoints secured, a modernized firewall, and $1.4 million in savings

Today, the client has enhanced network visibility and full control of all endpoints connecting to the network. This includes preventing unauthorized devices such as rogue network devices and removable media from accessing the network. The solution also automatically blocks attempted access from unpatched employee and third-party devices as well as from unregistered devices. Plus it enables easy and secure onboarding of new endpoints, and identification of all users logging into corporate assets. In total, more than 20,000 endpoints consisting of workstations, IoT sensors, and headless devices have been secured, and the client is now in compliance with FDIC network security requirements.

The client also has advanced firewall technology that is easier to administer and a more proactive security stance based on the latest best practices. This better positions them to identify, protect, detect, respond, and recover when faced with cyberthreats. Plus, they are benefitting from a consolidated firewall policy, fewer physical devices, and a five-year growth forecast for firewall throughput.

The firewall upgrade has delivered financial benefits as well. The organization saved $1.4 million through data center infrastructure consolidation.

Benefits:

- Advanced network visibility & access control
- Modernized firewall & proactive security
- Risk mitigation with minimal service interruption

$1.4 million
in hardware cost savings

Enhanced compliance

20,000+
endpoints secured