Bank Upgrades Security Ahead of Cross-Border Merger

Customer Case Study

UniCredit Slovakia simplifies guest access and lays groundwork for bring-your-own-device environment

EXECUTIVE SUMMARY

Customer Name: UniCredit Business Integrated Solutions (Societa Consortile per Azioni)

Industry: Finance

Location: Slovakia

Number of Employees: 1300

Challenge

- Enhance port security for guest users as visitor numbers rise
- Improve IT management capabilities with real time, granular reporting tools
- Prepare transition to bring-your-own-device environment when required

Solution

- Cisco Identity Services Engine integrated with Cisco Prime Network Control System
- Cisco Catalyst 3560X Series Switches with Cisco 5508 Series Wireless Controllers

Results

- Wired and wireless management integrated into single solution for OPEX savings through reduced hardware
- Guest portal makes visitor access quicker and easier to manage
- Full visibility of user and device profiles enhances security and efficiency

Challenge

UniCredit Business Integrated Solutions provides IT services to UniCredit Slovakia, a universal bank with a strong focus on retail banking. A subsidiary of Italy's UniCredit SpA, the bank is due to become part of a larger, cross-border unit through a forthcoming merger with another UniCredit subsidiary in the Czech Republic. The bank maintains a network of 75 branches, with two data centers and main offices in the Slovakian capital, Bratislava. UniCredit is seen as one of the strongest banks in central and eastern Europe, and the merger is intended to consolidate its market leadership.

To meet the need for comprehensive network security, UniCredit Slovakia first deployed a Cisco® Network Access Control (NAC) solution. With Cisco switches installed in its local area network infrastructure, the solution covered the bank's wired and wireless networks. It also secured some virtual local area networks (VLAN) that provide access to users from other UniCredit subsidiaries in the Czech Republic, Austria, or Germany.

When UniCredit Business Integrated Solutions carried out an internal security audit, the IT team decided on an upgrade from Cisco NAC to the more advanced Cisco Identity Services Engine (ISE). An all-in-one enterprise policy control platform that enforces compliance, enhances security, and simplifies service operations, Cisco ISE offers context-aware security with real time device profiling, on-boarding, and identification of corporate devices.

The solution would provide full port authentication, eliminating the burdensome task of manually setting up network access credentials for visitors. "The lack of expiry dates on guest access accounts was always a security threat, and the network administrator had to track them continually to check whether these accounts were still needed, which took up a lot of time," says Martin Pencev, head of IT at Unicredit Slovakia.

"We have more visits by foreign managers now, and they require corporate access. Using the Cisco ISE guest portal, we can flexibly and securely create temporary access for them."

Martin Pencev
Head of IT
Unicredit Slovakia

Solution

The new Cisco ISE security solution was implemented by local specialist ANECT and builds on a Cisco Borderless Network foundation. It supports a Cisco Open Network Environment (ONE) architecture for automated provisioning and fast deployment of services and applications. Deployed across the bank's fixed local and wide area networks, Cisco ISE covers all 75 branches. The solution also secures the Cisco Unified Wireless Network at its headquarters buildings in Bratislava, managed by a Cisco 5508 Wireless Controller in each data center, so executives can connect to the wireless LAN using notebooks with Cisco AnyConnect software.

To optimize visibility and control, the Cisco ISE security solution was integrated with the Cisco Prime network management platform. That combination brings together the wired and wireless domains with security policy management in a converged package for faster troubleshooting and more efficient network operations. This capability enables visibility into endpoint connectivity regardless of device, network, or location.

"A key aim for us was to take advantage of the profiling capabilities of Cisco ISE for a more secure and dynamic network without increasing management," says Pencev.

During the implementation phase, the IT team used some of its NAC hardware as a test environment for Cisco ISE, and has continued doing so as more ISE features are brought into play. Since Cisco ISE requires only two physical and two virtual servers, compared to the eight needed previously, the upgrade allows more efficient resource deployment.

Separate service set identifiers (SSIDs) were created for corporate users, onsite contractors, and guests. Corporate users have unrestricted access, with security assured wherever they work. Contractors working regularly on bank premises on domain PCs are in a different security group, and occasional visitors are authenticated via a dedicated guest portal.

Results

For UniCredit Slovakia, the key benefit of the Cisco ISE solution is that it enables unified security policy management and brings a significant uplift in security. "In a penetration test that followed the ISE implementation, the auditing agency was unable to make any headway and had to ask us for special access to continue testing," says Pencev.

The guest network is quicker and easier to manage: a matter of growing importance to the bank as the number of visitors from UniCredit subsidiaries elsewhere in Europe mounts up in advance of the planned merger. "We have many more visits by foreign managers now, and they require corporate access," Pencev says. "Using the Cisco ISE guest portal, we can flexibly and securely create temporary access for them."

In such a situation of growing cross-border staff mobility, the bring-your-own-device (BYOD) policy enabled by Cisco ISE, allied with the existing wireless infrastructure based on Cisco Aironet® 1142 Series Wireless Access Points and Cisco 5508 Series Wireless Controllers will provide convenience for those itinerant managers.

Meanwhile, greater ease of troubleshooting means a corresponding gain in operational efficiency, with less time needed to resolve incidents. Clarification of roles for the IT team is another valuable outcome. Setting up guest network access is now a simple matter handled by the firm's chief security officer, freeing the network administration team to get on with other tasks.

The new system has led to a major improvement in network management and visibility. Any endpoint can be deployed rapidly, with granular network access based on the endpoint type, including IP cameras, Cisco wireless access points, printers, and so on. And the single management pane allows the IT team to see at a glance all attributes assigned to any user.

"We can now create dashboards according to need. Cisco Prime lets us see the authentication profile for users and devices, so we know who is connecting to the network, where they are, and what devices they're using."

Martin Drozd
IT Specialist
Unicredit Slovakia

Cisco Prime Network Control System played a central role. "We can now create dashboards according to need," says Martin Drozd, an IT specialist at Unicredit Slovakia. "Our old monitoring system was less flexible and didn't show us everything. We now have all the necessary information displayed in one easy-to-reach place. Cisco Prime lets us see the authentication profile for users and devices, so we know who is connecting to the network, where they are, and what devices they're using."

Next Steps

The bank is enabling devices such as Androids, iPhones, and iPads to connect wirelessly at headquarters. It also plans to integrate the ISE platform with its existing mobile security solution from Cisco partner MobileIron. Meanwhile, Cisco TrustSec® is being looked at as the next logical step forward in the bank's BYOD readiness program. TrustSec works with Cisco ISE to enforce policies in a scalable manner, and reinforces data confidentiality with ubiquitous encryption between network devices.

For More Information

To learn more about the Cisco architectures and solutions described in this case study, please go to:

www.cisco.com/go/ise

www.cisco.com/go/prime

Product List

Security

- Cisco Identity Services Engine

Management

- Cisco Prime Network Control System

Wireless

- Cisco Aironet 1142 Series Wireless Access Points
- Cisco 5508 Series Wireless Controllers

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.**