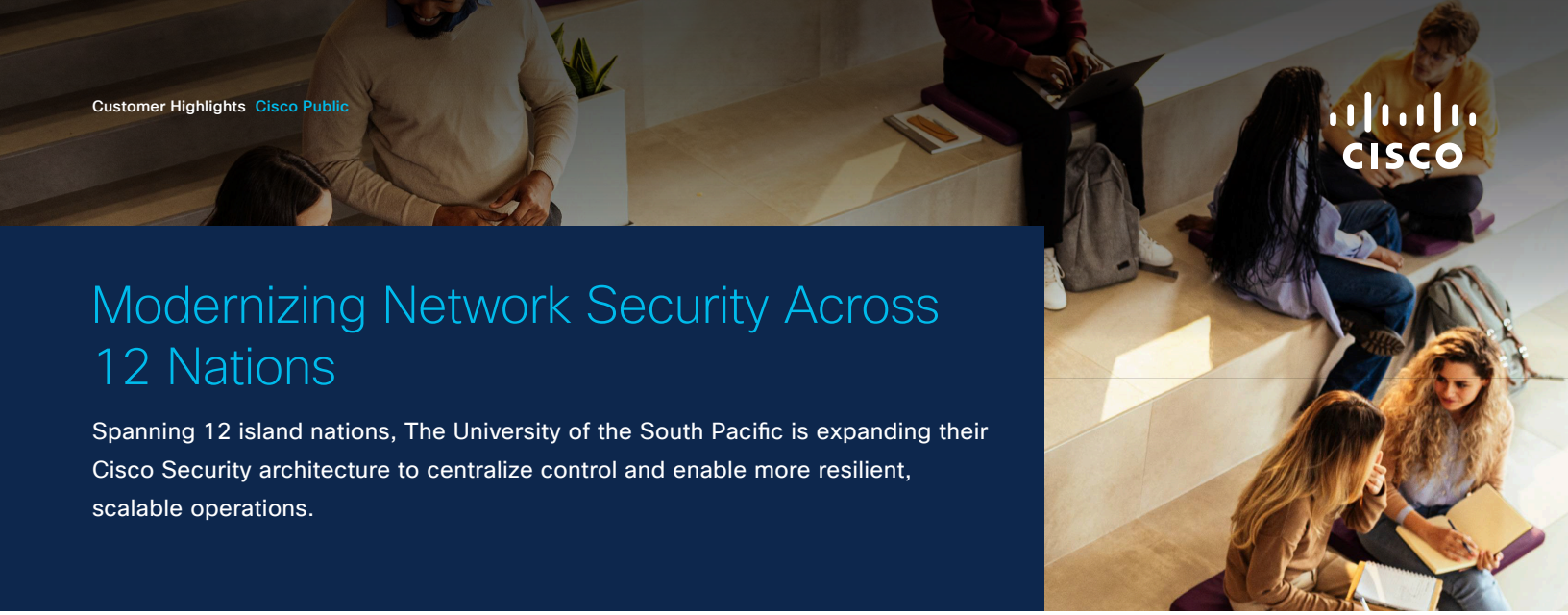

# Modernizing Network Security Across 12 Nations

Spanning 12 island nations, The University of the South Pacific is expanding their Cisco Security architecture to centralize control and enable more resilient, scalable operations.

USP
THE UNIVERSITY OF THE SOUTH PACIFIC

**Industry:**
Education

**Location:**
Suva, Fiji

**Organization:**
20,000 students and 1,700 staff

**Solution:**
Cisco Security Cloud Control
Cisco Secure Firewall 3140
Cisco AI Assistant
Cisco ISE
Cisco DUO
Cisco SD-WAN

## Connecting a region through security

Serving students across the vast Pacific Ocean is no small task. With campuses and learning centers across 12 nations and nearly 2,000 islands, The University of the South Pacific is one of the world's most geographically diverse higher-education institutions. From their central IT and cybersecurity hub in Fiji, the university supports over 20,000 students and 1,700 staff—delivering connectivity, learning platforms, and secure access across roughly 35 distributed sites.

Managing that scale with a small team has always posed challenges. The university's Enterprise Systems and Networks Infrastructure Manager, Edwin Sandys—who oversees networking, systems, cloud, and security—knew that consolidating tools and improving visibility was essential to protecting such a large, decentralized community. "When you're supporting 12 countries, you can't have 12 different security strategies," he explains. "We needed one architecture—something unified, cloud-managed, and intelligent."

The University of the South Pacific needed to simplify operations, reduce investigation time, and secure a highly distributed network with limited on-site IT resources.

1. Inconsistent visibility and fragmented defenses across campuses, cloud applications, and collaboration platforms
2. Disparate tools and manual processes limited the ability to quickly correlate user, device, and threat activity
3. Resource constraints across remote sites slowed response times and strained security operations

As the university's digital footprint grew, the need for a unified foundation became clearer. The team wanted to eliminate silos, strengthen visibility, and understand who—and what—was connecting to the network. They prioritized integration and ease of use, seeking an architecture that combined firewalls, cloud services, DNS protection, and identity-based access.

Cisco's integrated security portfolio aligned perfectly. Within two weeks, the team deployed Cisco Secure Firewall, configured Cisco Identity Services Engine (ISE) for identity-driven access control, and connected everything to Cisco Security Cloud Control for centralized policy and analytics.

"We used to spend 4 hours analyzing an incident—now it takes 15 minutes. Cisco Security Cloud Control gives us instant reports and visibility, so we focus on fixing problems, not chasing data."

– Edwin Sandys, Enterprise Systems & Networks Infrastructure Manager

© 2026 Cisco and/or its affiliates. All rights reserved.

This created an architecture that balanced simplicity with intelligence, enabling them to manage, monitor, and adapt policies across all campuses from a single interface. "We didn't just migrate—we modernized," Edwin says. "We rebuilt our rule base, cleaned up legacy configurations, and immediately gained visibility we'd never had before."

Today, Security Cloud Control serves as the university's command hub for firewall, health, and policy management. Real-time AI insights highlight redundant or misconfigured rules, helping them continuously optimize protections. "At a glance, we can see which rules are healthy or need attention," Edwin adds.

By consolidating multiple tools into one cloud-delivered platform, the university has built a security foundation that's easier to manage and designed to evolve—allowing less time spent troubleshooting and more time strengthening defenses across every campus, classroom, and connection.

## Turning threat hunting into threat resolution

Once the university unified visibility across their environment, the impact was immediate. What had been a complex, time-consuming process quickly became a streamlined, data-driven operation. The team can now detect, investigate, and resolve threats with far greater speed and confidence. "Before, an incident took half a day to analyze," says Edwin. "Now we spend that time solving issues instead of hunting for them."

With AI and automation embedded across the platform, investigation time dropped by 94%—from roughly 4 hours to just 15 minutes. Analysts can now trace activity across users, devices, and applications to understand exactly where an event originated and how it spread. "The integrations between our on-premises firewall management and cloud-based analytics make everything easier," Edwin explains. "It's honestly made a huge difference in how we work."

**94%**

**reduction in investigation time, unified visibility across 12 island nations**

Enhanced visibility also enables them to act faster and more precisely. When suspicious activity or malware appears, they can immediately identify the affected device and user—resolving issues before they escalate. The university's philosophy emphasizes collaboration and education rather than enforcement. "We're not trying to catch our users making mistakes," he says. "We're trying to help them. Our job is to educate and protect."

If malware is detected on a student device, the IT team brings them in for cleanup and shares best practices. For staff, targeted outreach campaigns have become foundational. When activity reports flagged risky device behavior, the team sent personalized guidance to employees.

The results were transformative. Internal threat activity declined sharply, and faculty began thanking the IT team for protecting them. "That was a turning point," Edwin recalls. "Security became something collaborative instead of reactive." This shift elevated cybersecurity from a technical function into a shared responsibility. Presentations to leadership now showcase complete visibility across the environment, strengthening confidence. "When we showed them how much data we can see now, they were amazed—and a little scared," Edwin jokes. Integrated systems have also created new operational efficiencies. The team now generates complete incident reports in minutes, and insight into traffic patterns and user behavior has revealed previously unseen threats—driving a more resilient, engaged security culture.

© 2026 Cisco and/or its affiliates. All rights reserved.

## Graduating from visibility to resilience

With people, process, and technology now aligned, the university has achieved an operational rhythm that's both efficient and resilient. Investigations are faster, awareness is stronger, and the entire community is more engaged in protecting its digital ecosystem.

"The visibility we have today changes everything," Edwin concludes. "We can see, understand, and act faster than ever—and that confidence extends to every campus, every classroom, and every person we support." The benefits of this transformation extend far beyond daily operations.

In their most recent regional cyber audit, the university saw a significant improvement in overall security posture—reflecting years of steady investment and process refinement. The team consistently shares these results with university leadership, showcasing measurable progress and deepening assurance in their security program. "That shift proved that our investment in Cisco solutions is paying off," Edwin explains. "We used to respond to incidents. Now we anticipate them." The security team has moved from reactive troubleshooting to proactive governance—continuously strengthening processes, refining policies, and engaging users across the region. What began as an effort to modernize technology has evolved into a program that enhances collaboration, transparency, and accountability across the entire university community.

## Harnessing AI and partnership for the future

Today, AI-powered capabilities within Cisco Security Cloud Control help The University of the South Pacific's analysts work smarter and faster. The system identifies redundant or unhealthy rules, flags configuration risks, and even guides junior engineers through best practices. "The AI actually teaches me how to ask better questions," Edwin laughs. "It's like having another expert on the team."

Automated analytics now handle much of the manual work once required to audit and optimize policies. Reports that used to take hours to build are now instantly available, enabling the team to focus on strategy, training, and long-term improvements. "We just open Security Cloud Control and everything's right there," Edwin says. "It's made us more consistent and far more efficient."

Beyond the technology itself, The University of the South Pacific has found lasting value in Cisco's authentic partnership and commitment to customer success. When the team encountered a challenge while testing new capabilities, Cisco acted immediately—mobilizing a cross-regional team of senior engineers and product experts to assist. Working side by side, they replicated the issue, conducted a comprehensive posture audit, and rapidly implemented a tailored solution that maintained seamless protection and operational continuity.

**Reducing risk with faster, more precise threat remediation:** AI insights and automation enable the team to detect, investigate, and resolve threats with greater speed and precision.

**Consistent security across every campus and cloud**: Cloud-based management empowers the university to scale, adapt quickly, and deliver consistent protection everywhere.

**Security resilience delivered in weeks, not months**: Improved visibility, proactive protection, and streamlined governance have quickly strengthened defenses and confidence.

## Leading Pacific security with Cisco Hybrid Mesh Firewall

With an integrated architecture firmly established, The University of the South Pacific is now preparing for the next stage of their journey—embracing Cisco's Hybrid Mesh Firewall solution and expanding their use of cloud-delivered security management.

© 2026 Cisco and/or its affiliates. All rights reserved.

By onboarding additional offerings into Security Cloud Control and further exploring key capabilities such as cloud-hosted policy enforcement and a unified AI Assistant across all Cisco Security tools, the university aims to manage every control point—campus, data center, and cloud—from a one, intelligent platform.

"Let me log into one place, ask one question, and see everything—from endpoints to the cloud," says Edwin. "That's the future we're heading toward." For the university, this evolution is about more than technology. It's about connecting and protecting communities across thousands of miles of ocean, empowering education through secure, reliable connectivity, and setting a new standard for cybersecurity across the Pacific.

"We've cut investigation times by 94%, doubled our security posture, and built a culture of awareness," Edwin concludes. "With Cisco, we're not just keeping up—we're leading the way for universities across the region."

"Cisco stayed in the trenches with us, they weren't just a vendor—they were part of our team. Cisco's engineers wanted to see us succeed. That level of commitment is rare—it's why we continue to invest in their solutions."

— Edwin Sandys, Enterprise Systems & Networks Infrastructure Manager

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 03/26