Cement Manufacturer Safeguards Wide Area Network Availability

TCL Group uses Cisco switching and security solutions to block intruders and maintain availability of manufacturing applications.

EXECUTIVE SUMMARY

Trinidad Cement Limited Group of Companies.

- Manufacturing
- Trinidad and Tobago, Barbados, Jamaica
- 1200

BUSINESS CHALLENGE

- Frequent network outages
- Lack of visibility into network security
- Risk of virus infection from guests and employees

NETWORK SOLUTION

- Comprehensive Cisco switching and security solution, including secure connectivity, intrusion prevention, security monitoring, and admission control

BUSINESS RESULTS

- No network downtime due to security issues or hardware failure
- Faster, more proactive response to potential security threats
- Much tighter control over internal and guest users on the network

Business Challenge

TCL Group is a leading producer of cement and concrete products with offices and manufacturing plants across the Caribbean. As a supplier of critical construction materials, timing means everything. So TCL relies on a sophisticated Oracle-based enterprise resource planning application to control sales, supply chain, financial reporting, HRMS and payroll at all locations. Since TCL's customers work under tight construction schedules, any inability to fill orders can cause major disruptions to their operations. That's why it's vital that TCL's network and applications are available and performing optimally at all times. A network security breach that were to bring down the primary data center in Trinidad—or the virtual private network (VPN) connections linking remote sites to the system—would be devastating.

"It would impact our financial operations including all our accounts payable and accounts receivable, as well as our human resources systems," says Khalid Rahaman, senior network administrator for TCL Group. "More importantly though, we rely on this system for order management, so we would not be able to sell our products to our customers."

Keeping the network and security systems online, however was becoming increasingly challenging.

"We had repeated failures on our VPN, and we were not getting the level of support we needed," says Rahaman. Over a period of four months, one of our critical links went down three times, each time for about 12 hours, during working hours."

TCL Group also suffered from a lack of visibility and control in the environment.

"We would receive complaints from employees that some applications were slow, but we had no means of pinpointing which devices were causing the problem," says Rahaman. "Our security monitoring was also very ad hoc. It relied on reviewing logs of events that had already occurred, so it was a reactive approach."

Part of the problem was the mixed-vendor environment, the result of the company's growth over the previous several years. Different locations used different network switches and firewalls, some of which were out of support and warranty. This impeded visibility and made it more expensive to support the network.

"We wanted to standardize the equipment across all our companies so that, at any point in time, any IT staff member would be familiar with the equipment at any location."

TCL Group also needed tools to monitor users in the environment more effectively, and to more tightly control guest access.

"We have a lot of vendors and consultants coming into the network with their own laptops, and potentially bringing viruses into our environment," says Rahaman. "We had no way to know who was on the network at any point in time. We needed a better way to control access."

> "The biggest benefit we've realized from this deployment is the stability of the Cisco devices. Since implementing the solution, we've experienced zero downtime related to a VPN failure, a security issue, or a network hardware failure."
>
> **—Khalid Rahaman, Senior Network Administrator, TCL Group**

Network Solution

TCL Group's leadership recognized that the company needed a more stable, secure networking environment to support its growing operation. They quickly zeroed in on Cisco to help them with the overhaul. The IT team was impressed with the reputation of the Cisco solutions, but even more impressed with Cisco's ability to work with them as a full business partner.

"Prior to coming to Cisco, we didn't have a relationship with our hardware vendor," says Rahaman. "We would just buy equipment and implement it ourselves. With Cisco, we have an account manager, an account team, and a support team to guide us through the entire process, from presales to implementation to ongoing support. We didn't have anything like this before."

Working with Cisco, TCL Group embarked on a project to update their switching and security environment. To serve as the core switching platform, the company deployed the Cisco Catalyst® 6500 Series Switch with Intrusion Detection System (IDSM-2) Module. The solution integrates full-featured intrusion prevention system (IPS) functions directly into the network infrastructure, where it allows TCL Group IT analysts to accurately identify, correlate, and block network threats. TCL Group also deployed the Cisco ASA 5500 Series Adaptive Security Appliance with the Advanced Inspection and Prevention Security Services Module (AIP-SSM) at the primary data center and remote sites. The platforms provide integrated firewall, VPN, and IPS services in a single solution.

"We are monitoring the IPS devices on a 24/7 basis," says Nickey Ali, assistant network administrator, TCL Group. "We can see active charts, graphs and logs of all of the information the IPS is collecting in real time. We can isolate any packet traversing our network and see an explanation of what it's doing and where it's going."

Recognizing the need to allow guests to operate in the TCL Group network safely, the company deployed Cisco Network Admission Control (NAC). The solution ensures that every user and device attempting to gain access to the network meets baseline security requirements, such as having up-to-date antivirus and operating system software, before granting access. To provide tighter control over internal users, TCL Group deployed Cisco Security Agent. The endpoint IPS solution monitors real-time operating system behavior in employee PCs to block malicious software and enforce compliance with corporate security policies.

To serve as the security monitoring command center of the entire environment, TCL Group uses the Cisco Security Monitoring, Analysis, & Response System (MARS). Cisco Security MARS provides a comprehensive picture of the security status of the network at all times, allowing the IT team to rapidly identify and block any suspicious activity.

TCL Group worked closely with the Cisco Advanced Services team to plan and implement the entire network and security implementation.

"For each component of the solution, we worked with a Cisco professional who was certified in that specific functional area," says Rahamn. "They had a detailed understanding of our long-term goals, and they even gave us ideas about how we could improve our environment moving forward. It was an excellent experience."

Business Results

Today, TCL Group's wide area network and IT security systems are more stable and secure than ever before, thanks to the company's robust Cisco network and security foundation.

"The biggest benefit we've realized from this deployment is the stability of the Cisco devices," says Rahaman. "Since implementing the solution, we've experienced zero downtime related to a VPN failure, a security issue, or a network hardware failure."

With Cisco IPS solutions and Cisco MARS, TCL Group is enjoying much greater visibility into the real-time status of the network environment, and more robust protection against potential threats.

"The ability to proactively monitor our environment has been a tremendous benefit," says Rahaman. "We're no longer reacting long after the fact. Now, when a potential issue arises, the Cisco MARS automatically notifies us via email, and we can immediately respond. We don't have to wait for a user to tell us there's a problem, and we don't have to wait for the next morning to review our logs to know something has happened."

The advanced packet monitoring and control capabilities also allow the TCL Group IT team to easily identify any degradation in application performance.

"In our Jamaica office, we used to receive complaints from users that their applications were running slow," says Rahaman. "Since upgrading the infrastructure, we're able to give them 'LAN-like' performance."

The security solution is allowing the company to continue working with critical vendors and consultants, while protecting the environment from malicious threats. TCL Group has been able to enforce much tighter control over the network.

"We receive alerts if, for instance, someone brings an infected USB memory stick from home and connects it to an office machine," says Rahaman. "We can pinpoint the user and assist that person in correcting any virus problems they may have on their home machine, as well as educating them about proper security policies. We can also tightly restrict the types of content users can browse on the Internet, and protect against malicious Web scripts. We have basically locked down our environment."

Finally, by integrating firewall, VPN, and IPS capabilities into a single, standardized solution, the Cisco ASA platforms are providing both capital and operational cost savings for the widespread, multinational IT organization.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switches

Security and VPN

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco IDSM-2 Intrusion Detection System Module for Cisco Catalyst 6500 Series
- Cisco AIP-SSM Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series
- Cisco AIP-SSM Advanced Inspection and Prevention Security Services Module for Cisco ASA 5500 Series
- Cisco ASA Secure Remote Access/VPN
- Cisco Monitoring, Analysis, & Response System (MARS)
- Cisco NAC
- Cisco Security Agent

"We have fewer appliances to manage, and when troubleshooting, we can now identify a single set of steps that analysts can use at any location," says Rahaman. "And, since it's a Cisco solution, it's supported by partners throughout the Caribbean, so we can quickly get local support whenever we need it. The annual support cost was also much less than what we were paying for our previous VPN solution. We've been extremely satisfied with our experience with Cisco."

Next Steps

In the coming months, TCL Group plans to further enhance their control over the network and security environment by deploying Cisco Security Manager. The solution will allow the IT team to manage security devices and configure security policies for every network device in the environment from a single console.

For More Information

To find out more about the Cisco ASA 5500 Series, Cisco NAC, and other Cisco security solutions, visit http://www.cisco.com/go/security.

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.

Printed in USA C36-542125-00 06/09