

## Secured a defense establishment by setting a “Golden Configuration” for all networking equipment

The customer is a defense organization which has more than 50 primary locations across the country. They wanted to set-up a command control center to ensure there was complete coordination between all the primary locations and the IT environment was made more secure.

### Company Overview

Customer has more than **50** primary locations across the country.

It manages national security and formulating defense policies.

### IT Environment

Network equipment from multiple vendors across multiple generations from the year 2000.

6000 older generation devices



### CHALLENGES



Older equipment lacked standard protocols, complicating integration efforts.



Limited global IBM TNCM installations caused resource shortages.



High Availability setup and security policies increased deployment complexity.

### SOLUTIONS



Utilizing driver expertise, two-way communication was established with legacy devices.



Enabled communication between 6000 legacy devices and TNCM console.



NCCM enabled golden rule configuration and tampering prevention workflows.

### IMPACT



Complete network security and visibility across all locations.



Automated compliance checks ensure continuous security and regulatory adherence.



Environment secured against unauthorized changes with time-stamped, tracked modifications.

## Case Study | Implementation Services

### "FORTIFYING DEFENSE WITH A GOLDEN CONFIGURATION FOR NETWORKING SECURITY"

The customer had network equipment from multiple vendors across multiple generations from the year 2000. The customer wanted to set up a golden configuration which could not be tampered with at the field level so that any kind of sabotage could be avoided.

To achieve this objective, they procured the IBM Netcool family of products from the IBM ITSM stack.

#### CHALLENGES

1. To be able to setup a golden configuration, all devices needed to be on a standard communication protocol. There were products which had been procured in the early years of the present century, they did not have standard communication protocols.
2. IBM TNCM has very few installs worldwide, so there not many experienced TNCM resources globally who can be sourced.
3. While IBM TNCM has connectors with present generation networking equipment from the popular vendors like Cisco, Juniper etc., it did not have connectors for old equipment like IPS, DSLAMs etc.
4. The customer wanted the implementation of the TNCM to be done in a High Availability setup so that there was no chance of failure or sabotage.
5. The setup had to ensure all the security policies could be implemented via the system

#### CHOOSING THE RIGHT SOLUTION AND MEETING THE DEADLINES

DCM has an extremely strong practice across the IBM Netcool family of products. We have a history of writing device drivers in the network space. We had IPs on all the major networking protocols - from X.25 to Wi-Fi to WiMax, USB2.0 and Bluetooth.

As mentioned above there were devices which did not support standard communication protocols. Using our experience of writing device drivers and networking protocols we were able to figure out two-way communications with the old DSLAMs, IPS, using MIBs being sent by these devices.



This helped in being able to get the 6000 older generation devices to communicate with the central TNCM console.

It was a complex project because of the variety of network devices from routers and switches to DSLMs etc. which needed to communicate via a single user console at the central location. The NCCM helped in being able to configure a golden rule for the devices and then build the workflow in case someone tries to tamper without a proper change approval.

#### THE BENEFITS

1. The customer has now got a secure “golden rule” based system for all their network devices and has a complete view across all locations in the country and across all network products of all generations.
2. The customer now has automated compliance checks for daily, weekly and monthly compliances.
3. The environment is now so secure so that no one can override the configuration at the field level and all changes are time stamped along with the complete change management process implemented.