New Zealand Department of Defence

Secure Collaboration with SharePoint Across Security Boundaries

Overview

Country or Region
New Zealand

Industry Defence

Also applicable to
Mining, Maritime, Exploration, Military Industries, Army, Navy, Airforce, Government

Customer Profile
The New Zealand Defence Force aims to promote the security of New Zealand, and to protect its people and its national interests.

Business Situation
The New Zealand Defence Force requires the ability to share information of a highly sensitive nature from the field and across the organisation in a timely manner; a specific challenge being the ability to move such information from a secure network to a deployed location.

Solution
With Myriad Technologies, the New Zealand Defence Force created a highly commended original solution.

Benefits

- Secure transfer of sensitive information across security boundaries
- Improved access to information allows more informed decision making
- Reduced demand on personnel time to manually replicate content
- Personnel can instead focus on tasks and activities that computers cannot automate

Myriad Technologies has a proven track record of developing and delivering award-winning solutions for military organisations. Myriad Technologies is the Microsoft Gold Partner selected by the Land Network Integration Centre to develop the Mission Secret Network. The New Zealand Defence Force (NZDF) Project is an extension of the information-sharing requirements across coalition forces. This has proven to be a valid platform for sharing information across nations and across security domains.

The NZDF consists of three services: the Royal New Zealand Navy, the New Zealand Army and the Royal New Zealand Air Force. The nation's armed forces adhere to three defence policy targets:

- to defend the country against a range of different threats
- to play a role in the security of neighbouring nations, and
- to take part in the global security front

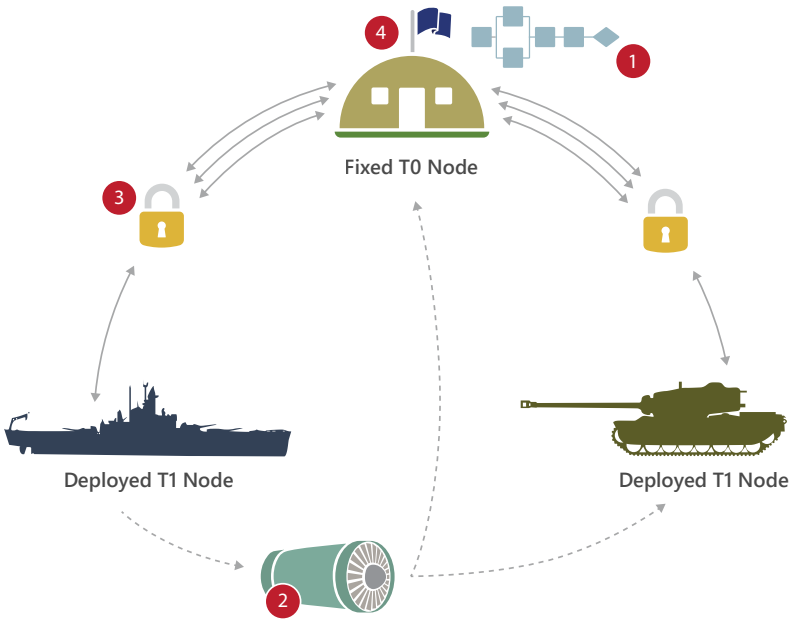
To fulfil the NZDF policy objectives the organisation conducts and participates in a number of exercises both at home and overseas. These exercises ensure the organisation is ready and prepared to respond to a number of different potential situations or crises.

The NZDF currently has over 11,000 active personnel and 2000 reserve personnel with small numbers deployed overseas on various tasks.

The Challenges

The NZDF encountered many challenges in order to fulfil the organisation's objectives. Most importantly is how information of a sensitive nature is securely distributed and shared around the organisation, especially to remote forces deployed in the field.

The NZDF overcame the specific hurdle of needing to share information from a secure network to a deployed location by employing one-way communication between two separated, air-gapped (physically not connected) networks. The process utilised by the NZDF to achieve the one-way communication was a manual operation that involved downloading the files, scanning them and re-uploading those scanned documents to the new



1. There is the ability to describe business processes that are then injected as structured collaboration and content elements within the node.
2. Provisioning of nodes is automatic. Subsequent replication is via the diode/ Turbine.
3. Security context and content is replicated across 'T' nodes to support collaboration and secure search for all content.
4. Nodes are provisioned and made 'aware' of each other to support secure collaboration content search across nodes.

Figure 1: Conceptual diagram of the sharing of information within the network of fixed (T0) and deployed (T1) Nodes.

network. To modernise these processes with streamlined automation would provide benefits to staff at all levels of the organisation, relieving them of time-consuming tasks that could otherwise be performed autonomously. Essentially, personnel would be allowed to focus on more intellectually-engaging duties.

While the NZDF's existing process met the organisational requirements around security, it was very time-consuming and inefficient. The people required to complete the work were often not available as it required individuals that had both a particular skill set and the necessary security clearance to handle the material. The brittleness of this business process directly impacted the organisation's ability to share information freely and effectively. Further, it reduced the organisation's capacity to make timely decisions based on the availability of accurate information.

The manual process described is antiquated in the commercial enterprise sector, but is still remarkably common in government organisations around the world that have specific security demands placed on their information.

Sharing information across the whole organisation presents a significant challenge and the solution implemented by Myriad Technologies is the first known technical solution to combine commercially off-the-shelf products to deploy a working solution in the field.

The Solution

Myriad Technologies, an Asia Pacific partner for iOra and a Microsoft Gold Partner specialising in content collaboration, was involved in the 'highly commended' original development and implementation of the Turbine through the Mission Secret Network. The work resulted in recognition at the Land Defence Australia Industry Innovation Awards, and for this reason, Myriad Technologies was asked to develop a solution, to assist in the implementation of, and to support the NZDF project.

The solution Myriad Technologies developed to overcome the challenge of needing secure communication between two separate domains involves three key components. These are:

The Turbine: The content replication challenge was overcome through a network appliance called the Turbine and a software package called Geo-Replicator. The Turbine sits between the two domains and forms a secure connection, allowing for one-way communication. At the centre of the Turbine is a data-diode that restricts the flow of traffic to a single direction, physically isolating the receiving domain from being able to communicate with the source domain.

Geo-Replicator: This is an industry-leading replication tool which is trusted by governments and defence organisations across the globe. Geo-Replicator provides guaranteed access to up-to-date business information, irrespective of connectivity and location. It works by collecting all the individual changes made in an environment and compressing them into a package called an 'amendment'.

Amendments are then transmitted, unpacked and deployed to the replicated environment. By only transmitting the individual changes rather than whole files and by using industry-leading file compression, amendment sizes are considerably smaller, ensuring they can be efficiently communicated across low bandwidth connections.

SharePoint: Developed by Microsoft, SharePoint is a content and collaboration platform already employed by the NZDF, as well as by many other governments and businesses across the globe. The organisation wished to continue using it while overcoming the challenge of replication of specific content across domains.

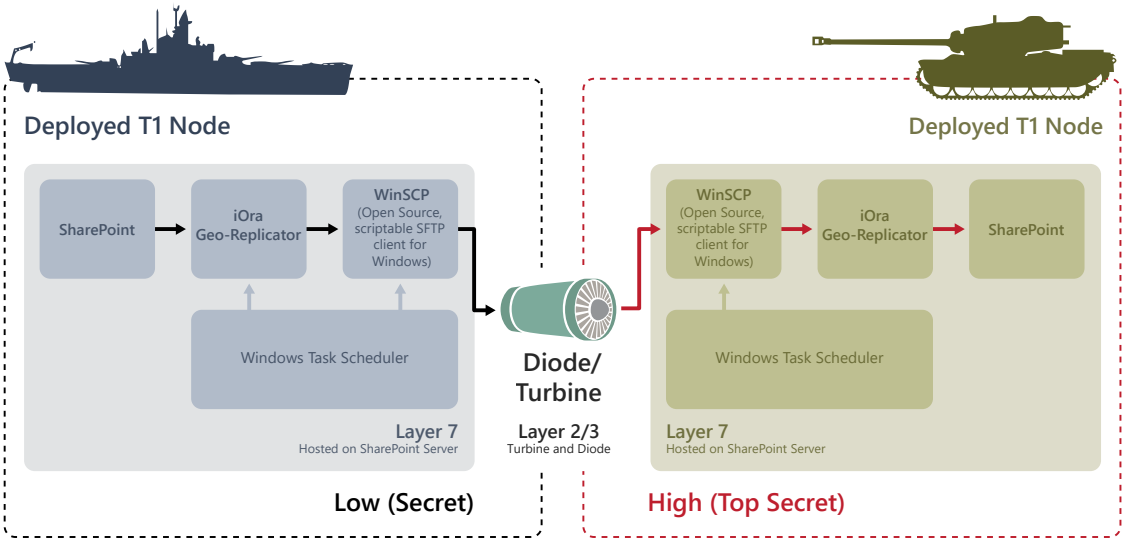


Figure 2: Conceptual diagram of the passing of information from one deployed T1 Node to another.

When combined, these three elements allow for secure one-way communication and replication of content from the secure to the deployed environment while ensuring the nonrepudiation of data.

Further information regarding the technical specifications and capabilities of the solution can be found in Myriad Technologies' cross-domain replication white paper.

The Implementation

The solution was designed for deployment across the entire NZDF organisation, with the original implementation created to be a test case; thus, it was deployed as a part of a live field exercise. Before the live exercise was conducted, a two-week rehearsal was held with one week of set-up prior, to test the system and ensure smooth operation during the live exercise.

Both the implementation and the solution's deployment were successful during the rehearsal, demonstrating that the process could be easily automated. The live exercise further enhanced the deployed solution by identifying key unforeseen operational challenges to further refine the final solution.

In summary, the primary project objective - to develop a solution that replaced the manual process of transferring content between domains - was a success, which ran on time and within budget.

The Benefits

The test case was successful in proving the potential for the organisation, for example by improving the transmittal of time-sensitive information and by freeing-up scarce and critical resources. These potential benefits could be further realised if the solution was to be implemented more expansively.

Moreover, the exercise formed a Proof of Concept, confirming that automating the information replication process across two disparate domains to streamline the sharing and disseminating of critical information is possible. This has helped illustrate various business benefits, including reducing the human error factor, leading to a better quality outcome overall, than the manual approach. Further, staff are freed from mandraulic tasks to focus on more intellectual work, for example information management, assessment or situational awareness.

The solution reduces the need for specialist personnel resources by removing the need to manually replicate content between domains, a tedious process which is extremely time-consuming and demanding of a specific skill set. In addition, decision-making and other activities can occur more effectively by providing defence personnel with their required information in a timelier manner.

The time-saving benefits of the solution translate into cost savings for the organisation in the long-run. The solution developed allows for government and defence organisations who are typically heavily restricted by information security to also enjoy the productivity-boosting benefits of collaboration and content management systems in a secure manner.