Organisations can transfer files between networks using USB sticks, but this is an insecure and inefficient practice. Using data diode and data guard technology can significantly improve the speed, control and security for organisations in sharing files across its different network domains.

**THE CLIENT**

A European multi-partner organisation.

**THE CHALLENGE**

The client needed to enable its staff to share files from one segregated network to another segregated network in an efficient and secure manner.

Previously the organisation was relying on the transfer of data using USB sticks and had experienced instances of leakage of sensitive information.

To bring in more control, manual reviewing procedures could be carried out using USB sticks, but this labour-intensive process is slow and cumbersome.

Also, this kind of review is usually carried out on an ad-hoc basis, so there is no management or audit of these activities, and it is easily possible to circumvent the manual process. In addition, ongoing manual reviews bring additional workload for users releasing files, and inconvenience for line managers and information security managers within organisations.

Our client needed a more automated process to enable users to transfer files easily; allow line managers to check documents more efficiently, and in a manner that fitted with their daily or weekly schedule.

The client had also taken the decision to increase the classification of one of its networks, resulting in an additional level of security being required. So, the timeframe for the delivery of a new solution was critical to meeting this upcoming change.
THE SOLUTION

Nexor worked with the client on a two-stage solution. The first stage was to install a method of flow control between the two networks that negated the use of USB sticks. The second stage was to bring in a validation check that added additional control in advance of the security classification of one of the networks being raised.

Nexor designed and implemented a data diode-based solution, which replaced the USB stick transfer process. The Nexor Data Diode enforces traffic flow entirely in one direction within a physically separate, hardware-only, data diode device. This is connected to proxy servers both upstream and downstream via fibre cables.

The solution uses a pair of Nexor Data Diodes; one to transfer information from the low-side (administrative) to the high-side (secure); and then another data diode/proxy combination for files to flow the opposite way from the high-side to the low. A minimal risk of a two-way data flow exists, but this is controlled by using two separate connections, each with independent data flows, protocols, and security policies.

For the second phase of the solution Nexor deployed its high assurance, cross-domain guard platform, Nexor Guardian. This provides a network share folder that users can easily drag and drop their files in, for submission into the Nexor Guardian validation framework.

Nexor Guardian protects the confidentiality of an organisation’s information by automatically validating that data is conformant and complies with the security policy of the protected domain. It ensures that an electronic exchange can only pass from one domain (secure network) to the other domain (administrative network) via a trusted path, and via a deep content filter to check it is releasable.

Nexor Guardian includes the option to implement a man-in-the-loop release control mechanism to authorise the export of files to the lower classification network. We worked with the client to produce an enhanced workflow that ensured an efficient, user friendly and secure process for both users and authorisers.

Once the file is submitted to Nexor Guardian, authorisers are notified that files are waiting for their review at configurable times, such as morning, lunchtime, or every day, so as not to interfere with their work. Once authorised, Nexor Guardian notifies users when files have been released so that they can be accessed in the administrative network without delay.

To simplify authorisation, the manual release capability uses an Active Directory structure to enforce access control rights for all submission and validation activities.

All activities on Nexor Guardian are fully audited to provide complete oversight of all information transfers out of the domain. It provides a seamless transfer of files for authorisers and users, whilst improving working efficiency and reducing the risk of bypass.
TRUSTING THE SOLUTION

The solution uses Nexor’s industry-leading SIXA® portfolio of trusted information exchange products, which are based on our Secure Information eXchange Architecture (SIXA). The portfolio consists of configurable modular building blocks that follow best practice from the National Cyber Security Centre (NCSC), the UK National Technical Authority, for the import and export of data across security domain boundaries.

In addition, all of the proxy appliances used were Common Criteria certified to Common Criteria EAL4+, while the Nexor Data Diodes are assured to Common Criteria EAL7+, the highest certification possible.

The Nexor software in the solution was developed using our CyberShield Secure® development process that conforms to Microsoft SDLC, CMMI and TickITplus standards.

The solution met the requirements of the organisation’s internal accredditor, and was subjected to a third-party penetration test. This meant that the regulatory authority of our client was satisfied that a suitable solution had been deployed to overcome the previous data leakages and meet the new security requirements of the raised classification level.

THE IMPACT

Both stages of the solution implementation were initially trialled with a small group of users for testing but were then quickly adopted for all users of the two networks. The solution is scalable to cope with rising demand within the organisation.

The solution has completely stopped the usage of USB for file transfers between segregated networks, as all the USB ports are now disabled on devices connected to the higher security level network. This means that the risk of sensitive data leakage is minimised.

Efficiency has also improved as file shares from the low to the high-side are now instant. The speed of transfer from the high to low-side depends upon the manual release of the file but the solution has been designed to fit into the workflows of the organisation and not have any bottlenecks.

By using a data guard to validate the release of information, the organisation has increased its security. The manual release function adopted has also given them the oversight the client required.

The Nexor cross-domain solution has enabled our client to carry out its business activities as it wanted to, but without compromising on security. Our client is now looking at adopting the same, or similar, cross-domain solutions for connecting its secure network into other networks across the organisation.

NEXOR CAPABILITIES

Nexor provides solutions to get information into and out of secure networks. This enables organisations to perform more efficiently and effectively. The connection of secure networks is achieved by using people, process and technologies that align to best cyber security practice established by national authorities.