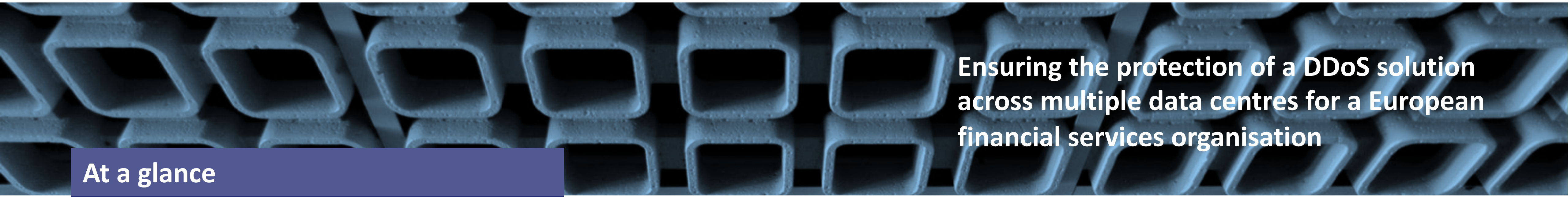
An NCC Group case study

Ensuring the protection of a DDoS solution across multiple data centres for a European financial services organisation

Client confidential



Ensuring the protection of a DDoS solution across multiple data centres for a European financial services organisation

At a glance

Organisation
European financial services organisation

Industry
Finance

Challenge
Assess the suitability of the client's DDoS mitigation services across multiple datacentres

Solution
NCC Group deployed a network layer DDoS test, utilising almost 1,000 bots across two hours

Results
The client's mitigation services, people and processes withstood the attack

Short Summary

NCC Group were approached by a European financial services organisation to provide assurance of its people, processes and mitigation services.

Specifically, the client wanted to ensure that the platform could appropriately detect, alert and scrub malicious traffic. The main objective for the DDoS exercise for the client was to assess the ISP's DDoS protection of multiple data centres. The test proved successful and the client was able to withstand the simulated and controlled DDoS attacks.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever- evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

Client confidential

Summary

NCC Group were approached to provide assurance of the abilities of a European financial organisation's DDoS mitigation platform. The client wanted to ensure that the platform could appropriately detect, alert and scrub malicious traffic. The main objective for the DDoS exercise for the client was to assess the ISP's DDoS protection of multiple data centres.

Challenge

The financial services organisation enlisted NCC Group's support in providing a confirmation of defence in depth, testing an automatic mitigation service against one data centre to gain confidence, and to ensure that service level agreements were met to monitor. detect and mitigate any attack.

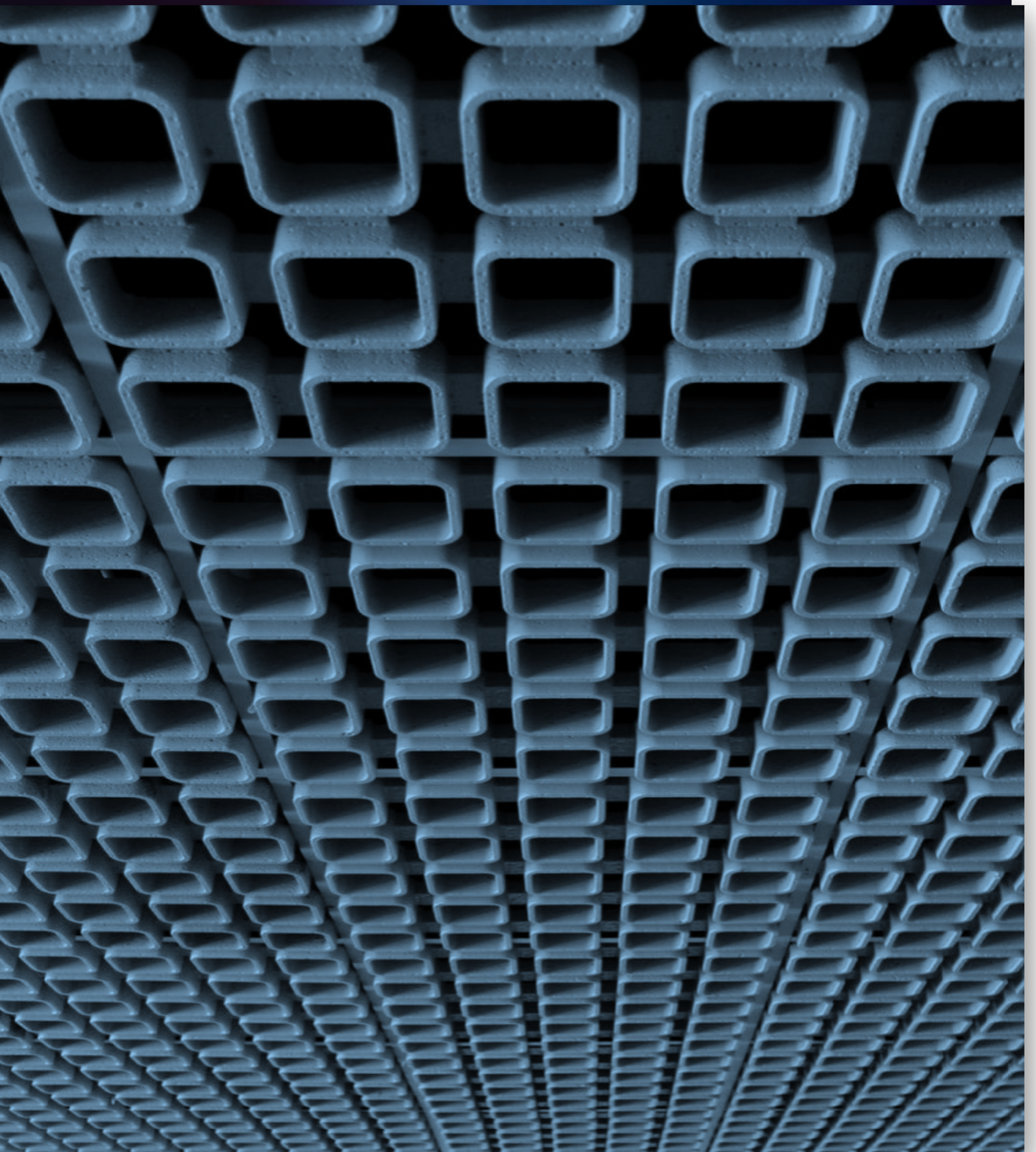
A second test was requested to run DDoS testing across the protections, processes and procedures of the client's other datacentres.

Solution

The network layer test was conducted over two hours. The attack types were TCP-SYN (500 bots, approximately 450 Mbps) and a mixture flood of SYN flood and UDP flood bots (450 bots, approximately 480 Mbps). The TCP-SYN floods are designed to operate by configuring each bot to repeatedly send SYN requests to end targets in an attempt to consume as many connections as possible. These TCP handshakes are never completed and left in a pending state, thus eventually preventing new and possibly legitimate connections being made to the server.

The mixture flood was aimed at testing the mitigation's capability to handle more complex multi-vector attacks against its infrastructure with a high bandwidth requirement. The UDP flood bots leverage the simplicity and speed of the UDP protocol whereby the botnet sends a high load of UDP traffic with the intention of trying to either overload the target's resources or consuming the target's available network bandwidth. The UDP packets contained random messages averaging 1,400 bytes in size.

NCC Group were generally unable to impact the targeted services run by the organisation, the mitigation detected and eliminated attack traffic quickly and efficiently. There was a loss of connectivity to the external firewall and the organisation was able to effectively correct this during the testing.



Results

The test provided the client with the necessary assurance it needed in the technology, processes and people in a safe and controlled environment. It also demonstrated to the organisation that its team is able to react quickly and effectively in a real life attack scenario. Due to the success of the testing, the client requested NCC Group to run further tests across its data centres which also proved to be successful.