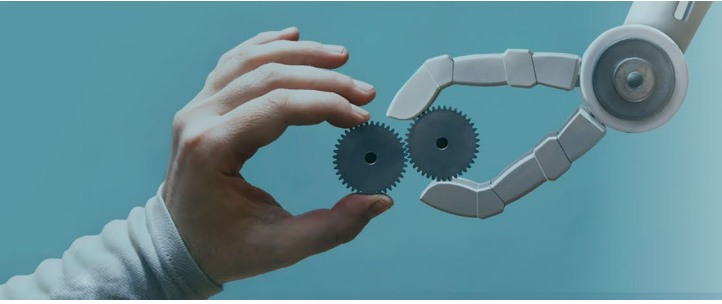

FLINT
Empowering Through Experience

# Next Gen Firewall Policy Implementation with OBS

## Business Challenge

**Orange Business Services (OBS)** were looking to provide **secure internet access across their business.** The level of access should be defined by end-user role and defined at a policy level.

Due to the specialised skills required to implement this solution, OBS was looking for a partner to provide the end-to-end implementation of this service within a **predefined budget and timeline.**

## Customer's Technical Requirements

Deploy centralised Internet access for users from different locations.

Implement Next Generation Firewall (NGFW) policies on DC firewall (Cisco FTD 9300) and Edge firewall (Checkpoint 23000) according to existing security requirements, adjust current policy to **optimise performance of security appliances.**

Deploy a pair of ISE-PIC appliances for user identity.

## Scope of Work

The Flint team executed the following steps from a mutually agreed statement of work:

1. Create firewall chain in LAB environment with integration to corporate AD and ISE-PIC appliances.
2. Adjust the existing Internet access policy with new NGFW capabilities and additional requirements.
3. Organise & group rules within the Internet Access Policy to avoid potential challenges with security efficacy and device performance.
4. Provide operational procedure to manage any futures operation changes.
5. User-identity service is handled by High Available (HA) pair of ISE-PIC appliances with PassiveID feature.
6. Primary ISE-PIC node polls preconfigured set of domain controllers by WMI call and get required user to IP address mappings.
7. User-identity information replicated to FirePOWER Management Center using PxGrid service with upcoming sensors updated in real-time.
8. FTD captive-portal NTLM authentication deployed as failback authentication method. In case user to IP mapping has expired and not updated, problems with PxGrid service, etc., user seamlessly authenticated by NTLM.
9. As part of solution deployment, Firepower FTD and FMC appliances were upgraded to the latest recommended software version, including some major bug fixes and hardware SSL acceleration support.
10. Install the latest hotfixes to the Checkpoint cluster.
11. Deploy Firewall policies to appliances at the first maintenance window, where some test users from different locations were switched to the new topology.
12. Prepare detailed migration plan for each location with failback scenario was reviewed and approved with the customer.

## Customer Impact

The solution has provided a **fully unified approach** for user Internet access including NGFW policies executed by a chain of both Cisco Firepower and Checkpoint Firewalls. Only authenticated and authorised users now have access to an approved set of internet resources. The project was **implemented on time and within budget**.

Want to know more? Visit [www.flint-international.com/our-services](www.flint-international.com/our-services)

+44 1923 677 733
www.flint-international.com
contactus@flintmail.com