# OFAC Black List Implementation

## Synopsis

In compliance with office of foreign asset control mandates, (TSST) Trust and Site Security Team has informed us to block six countries from reaching our sites in US and abroad. The black list in the gateway firewalls will intercept any incoming Internet communication from Syria (SY), Iran (IR), Ukraine (UA), Cuba (CU), Sudan (SD), and North Korea (KP.) This will also include DNS name resolution requests.

### Sites affected

This is involving all the sites our team supports, private and public cloud.

- Aurico hosted in Rackspace. Done for SY, IR, UA, CU, and KP on 06/23/2017
- Scheduled for the week of 07/17/2017
  - Aurico we need to block Sudan that was added to the original request to block only five countries
  - QTM Suwanee Quality Technology private data center, firewall PaloAlto
  - QTW Suwanee Private data center, firewall PaloAlto
  - CHI Elk Grove Equinix Private data center, firewall PaloAlto
  - ASH Ashburn Equinix Private data center, firewall Fortinet
  - Broadbean KCOM private datacenter in GS2 UK, firewall Fortinet
  - Broadbean KCOM private datacenter in GS1 UK, firewall Cisco ASA

### Impact

Since the list is not 100% accurate, we have to be mindful about blocking some legitimate users, such as the contractors from the black listed countries. We will be watching this with CS customer support team for customer complaints and adjust per request basis. For this purpose, we will be keeping a white list to override the black list.

### Implementation Steps

We will use the same testing process done for Aurico. The implementation is easy. On Cisco ASA we have to download the country list compile it into Cisco ASA format and then upload it into object that later will be applied to the black list policy. The rest of the firewalls have dynamic Geographical IP list grouped by countries.

- Add countries to a black list object
- Add new deny policy
- Apply object the object to the policy
- Test using proxy from the six blocked countries
- Check to see if the policy is dropping traffic