Superuser Whitelisting

Currently, L'Oreal allows employees and contractors to use their own devices.

To allow Users to connect to Snowflake, we will allow a subset of users to connect from the open internet (0.0.0.0/0 IP).

To manage who will have that privilege we will create a stored procedure that will whitelist all users who are associated with a determined AzureAD group (in our case, _TECH_OPEN_INTERNET_ACCESS_ROLE) and any role higher in the role hierarchy.

NOTE:
We will not go higher than one role in the heirarchy

```
CREATE OR REPLACE PROCEDURE OPEN_IP_ADMIN_SP(
    DRIVING_ROLE varchar,
    NETWORK_POLICY varchar
  )
  RETURNS varchar
  LANGUAGE JAVASCRIPT
  COMMENT = 'SP used to whitelist the users associated to a set of roles'
  AS
$$
//Creating Variables
let v_driving_role = DRIVING_ROLE;
let v_network_policy = NETWORK_POLICY ;

//Sql command to join Account usage user to role, to list of users
let v_return_users_sql = `with hierarchy as
            (select
                  name as parent_id ,
                  name        as child_id ,
                   1 level,
                  array_construct(child_id) path,
                  name as top_role
           from   snowflake.account_usage.roles  r
           where deleted_on is null
           union all
           select
                  pc.grantee_name ,
                  pc.name ,
                  h.level+1 level ,
                  array_cat(h.path, array_construct(pc.name)) path,
                  h.top_role
          from snowflake.account_usage.grants_to_roles pc
          join hierarchy h
          on h.child_id = pc.grantee_name
          where not array_contains(pc.name::variant ,h.path)  --eliminate circular references
          and granted_on = 'ROLE'
          and granted_to = 'ROLE'
          and privilege = 'USAGE'
          and deleted_on is null)
          select distinct 'ALTER USER "'||GRANTEE_NAME||'" SET NETWORK_POLICY '||'` + v_network_policy + `'
          from hierarchy h
           join snowflake.account_usage.grants_to_users gtu
              on h.top_role = gtu.role
          where CHILD_ID='` + v_driving_role + `'
          and DELETED_ON IS NULL
          and GRANTEE_NAME like '%@%'
          ;`;

//Execute sql to get list of distinct Users
let v_return_users =  snowflake.execute( {sqlText: v_return_users_sql} );

//Looping through the Users
 while (v_return_users.next()) {


  let v_user_whitelisting = v_return_users.getColumnValue(1);
  snowflake.execute( {sqlText: v_user_whitelisting} )

 }

 return "Success"

$$;


call OPEN_IP_ADMIN_SP('_TECH_OPEN_INTERNET_ACCESS_ROLE','BREAKGLASS_POL');
```