IAM Policy to Restrict Scope of Privileges

Restrict Request Source to Cornell Campus IPs

Here's a simple IAM policy that you can add to any existing IAM Group, User, or Role to ensure that the role is only utilized from a computer that has a Cornell public IP address.

Add this policy as an inline policy attached to any IAM User, Group, or Role. This policy cannot be used alone. The IAM User, Group, or Role must ***also*** be granted the privileges you want the user/group/role to have. See also https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "aws:SourceIp": [
                    "128.84.0.0/16",
                    "128.253.0.0/16",
                    "132.236.0.0/16",
                    "192.35.82.0/24",
                    "192.122.235.0/24",
                    "192.122.236.0/24"
                ]
            }
        }
    }
}
```

Restrict Scope of EC2 to One AWS Region

Add this policy to a managed policy, user, role, or group to restrict the scope of EC2 activity to just us-east-1 AWS region. Since it is a DENY rule, it would override any ALLOW rules in the policy, user, role, or group.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            },
            "Action": "ec2:*",
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

Attribute Based Access Control (ABAC)

Restricting access to resources based on tag values of the principal (IAM user or role) may be beneficial in certain scenarios. Please review our ABAC documentation for more detailed information.