Milestone 4 Goal

Automate creation of VPN server in EC2 Instance, using AWS CLI commands and shell scripts.

Solution

1. `create-security-group.sh`: creates a security group and prints the newly created security group ID. This script requires these environment variables: ec2sg: the security group name, vpcid: an existing VPC ID, and awsprofile: an aws profile name.
2. `update-security-group-ingress.sh`: updates Ingress rules in the new security group. This script requires these environment variables: ec2sgid: the newly created security group ID and awsprofile.
3. `create-ec2-instance.sh`: creates EC2 instance and then installs WireGuard packages and prepares WireGuard template configuration. This script requires these environment variables: ec2sgid, ec2ami, myuserkey, subnetid, ec2sgid, az and awsprofile.
4. In the EC2 Instance:
    a. Edit /etc/wireguard/wg0.conf file to update keys.
    b. Edit /etc/sysctl.conf, to enable ip_forward.
    c. Start WireGuard, using sudo systemctl start wg-quick@wg0.
5. In the Windows laptop:
    a. Edit WireGuard configuration, to update keys and VPN server endpoint.
    b. Activate VPN Tunnel.

Summary

The VPN Server is created with significantly automated shell scripts containing AWS CLI commands. This now helps to create/re-create new VPN Server easier and faster.