Milestone 3 Goal

Showcase the file sharing between remote EC2 Instance and local laptop, which is done securely through VPN server configuration on server and client.

Solution

Configure EC2 Instance as VPN Server

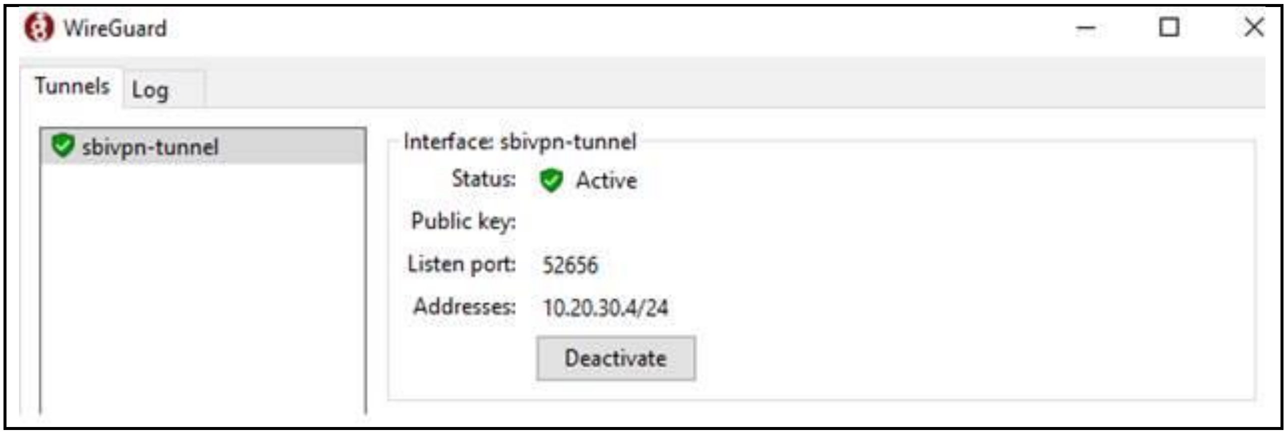
In EC2 Instance Ubuntu, create or update /etc/wireguard/wg0.conf

```
[Interface]
Address = 10.20.30.1
ListenPort = 41820
PrivateKey = <SERVER PRIVATE KEY>
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

[Peer]
# Name: windows-client
PublicKey = <CLIENT PUBLIC KEY>
AllowedIPs = 10.20.30.4/32
```

Configure Laptop as VPN client/peer

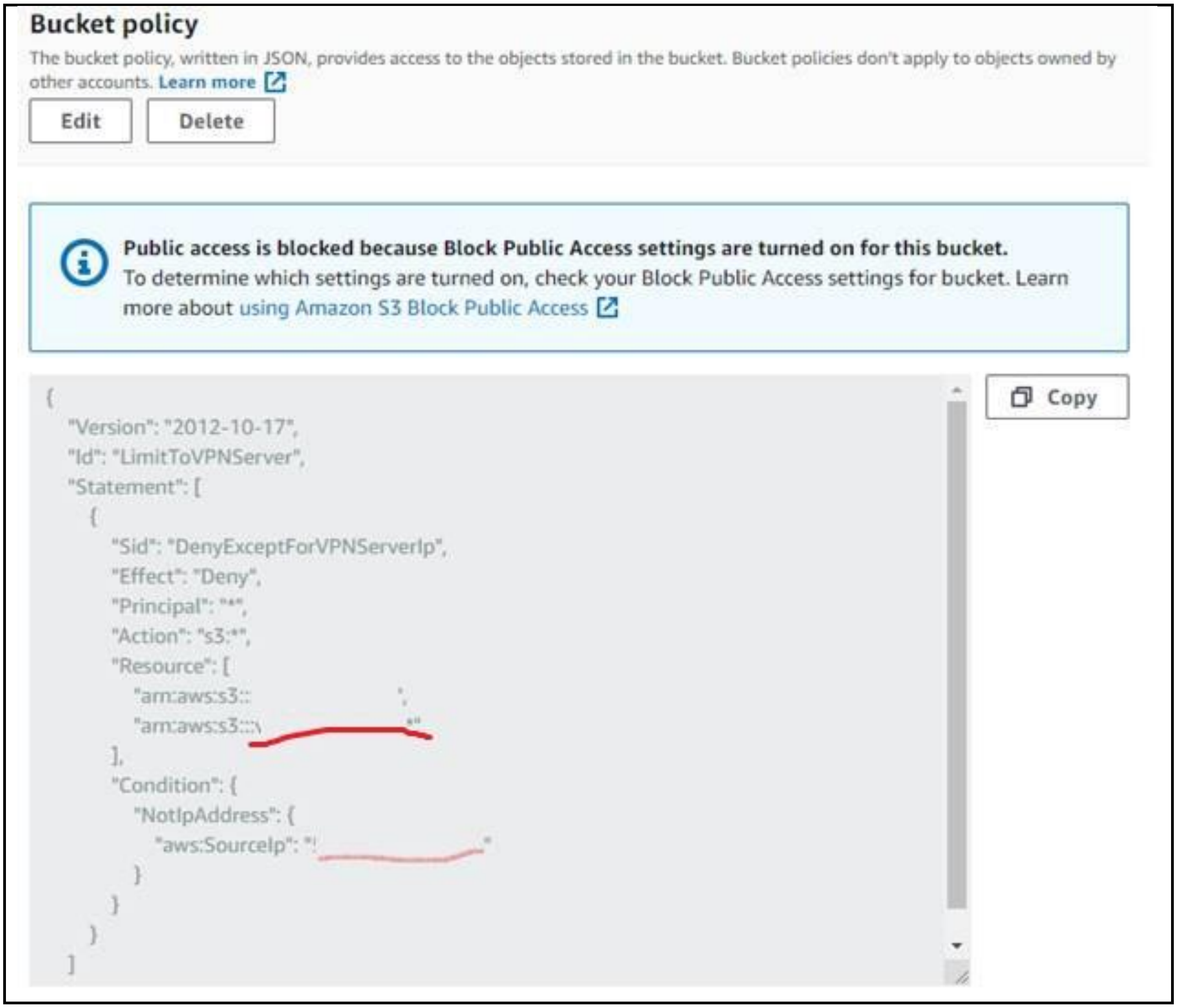
In Windows laptop, create or update WireGuard Tunnel



Interface: sbivpn-tunnel
Status: Active
Public key:
Listen port: 52656
Addresses: 10.20.30.4/24

Apply bucket policy on S3 Bucket

In the AWS Management Console, open the S3 bucket to be secured with VPN connection. Apply the Bucket Policy to deny access except for VPN Server IP.



Bucket policy

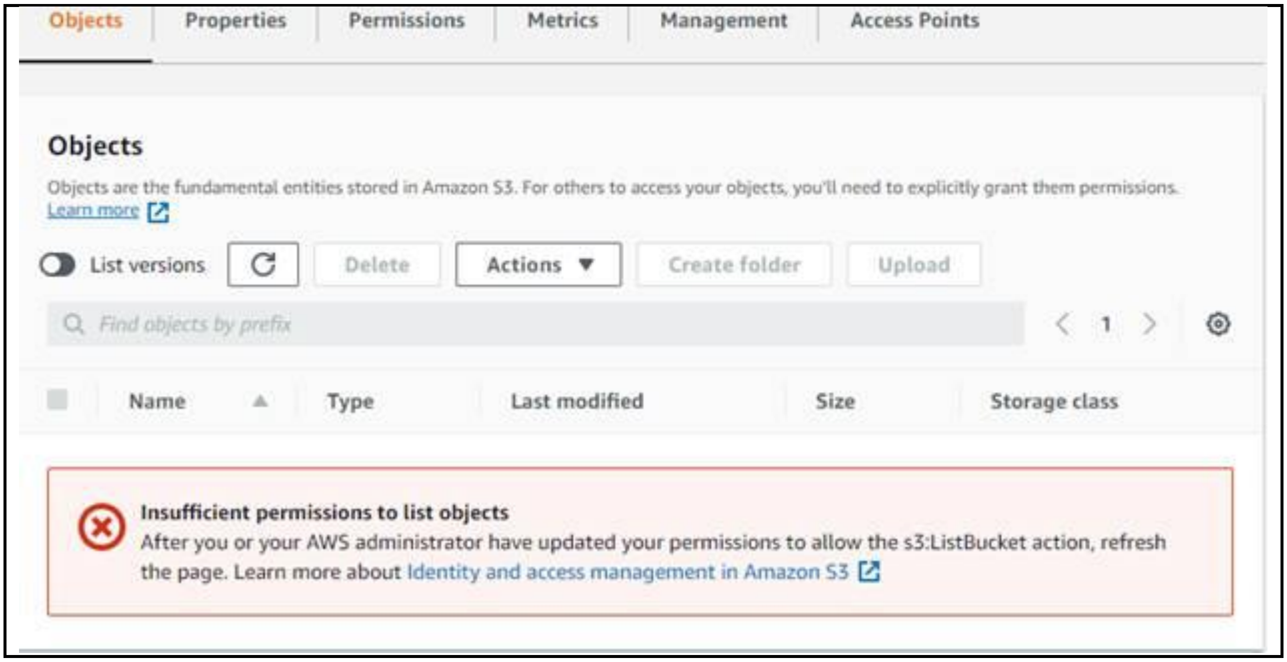
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket.
To determine which settings are turned on, check your Block Public Access settings for bucket. Learn more about using Amazon S3 Block Public Access

```
{
  "Version": "2012-10-17",
  "Id": "LimitToVPNServer",
  "Statement": [
    {
      "Sid": "DenyExceptForVPNServerIp",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::[redacted]",
        "arn:aws:s3:::[redacted]*"
      ],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": "[redacted]"
        }
      }
    }
  ]
```

Test accessing S3 bucket from laptop, without VPN connection

In AWS Management Console, open Amazon S3 and the bucket with limited policy (see earlier step), and I can’t see the S3 objects.



Objects

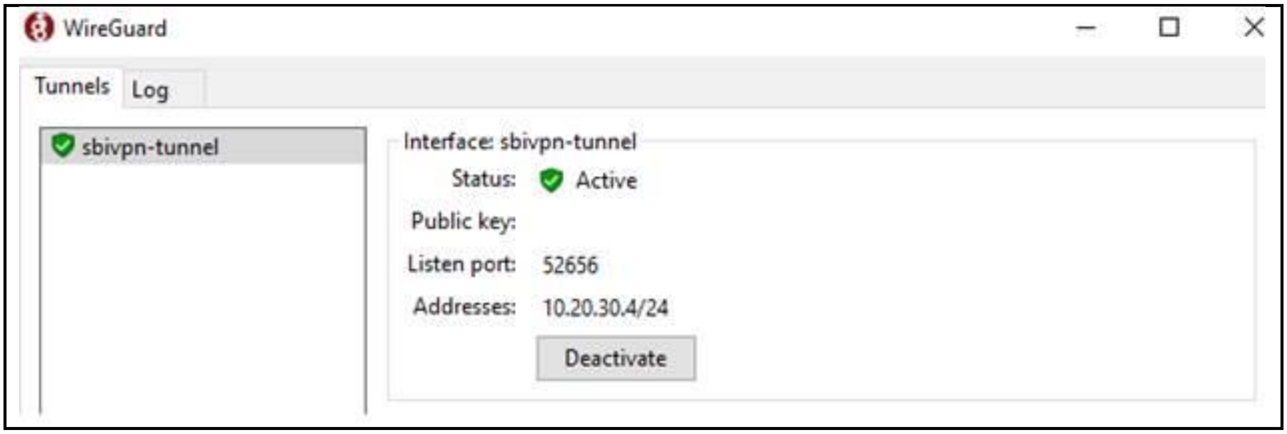
Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Insufficient permissions to list objects

After you or your AWS administrator have updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

Test accessing S3 bucket from laptop, with VPN connection

In the laptop VPN WireGuard, I first ensured the VPN tunnel is active.



Interface: sbivpn-tunnel

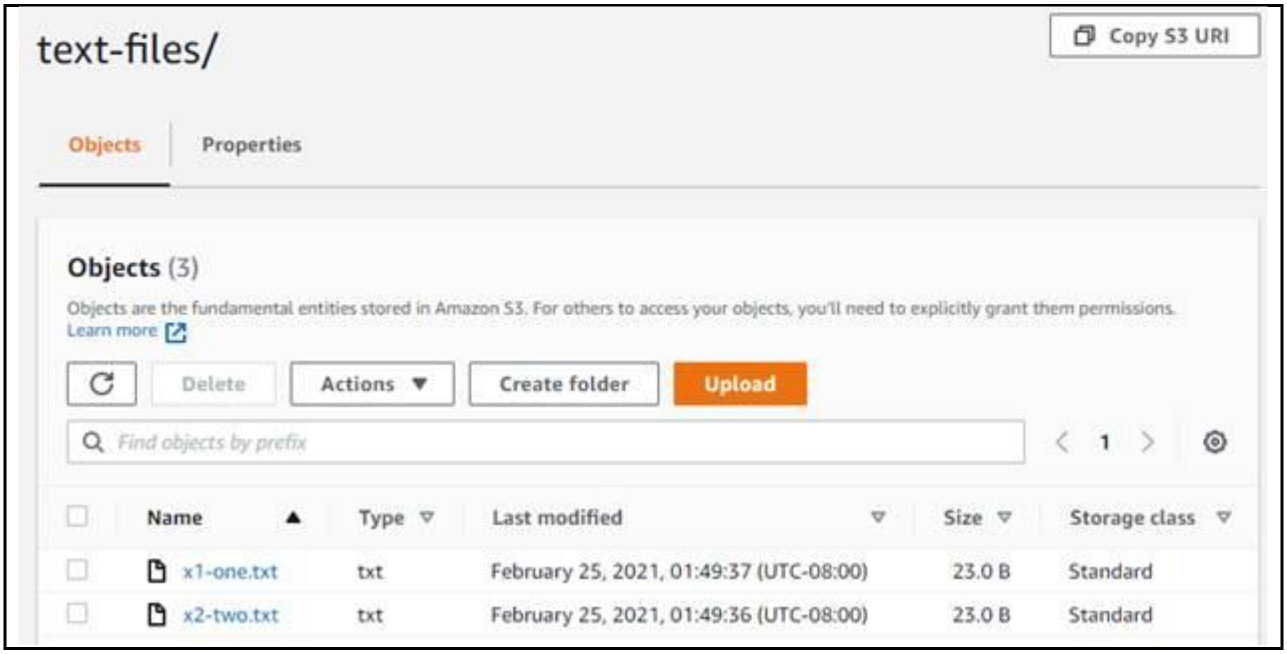
Status: Active

Public key:

Listen port: 52656

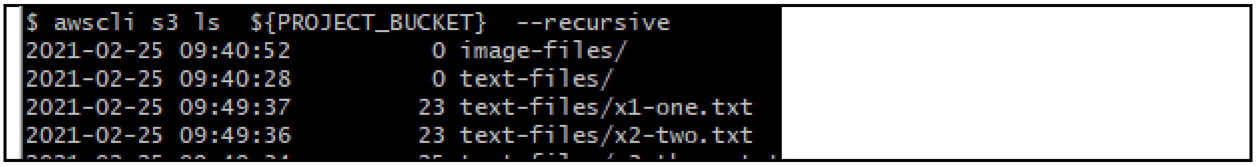
Addresses: 10.20.30.4/24

In AWS Management Console, open Amazon S3 and the bucket with limited policy (see earlier step), and I see the S3 objects.


text-files/
Copy S3 URI
Objects
Properties
Objects (3)
Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions.
Learn more
Delete
Actions
Create folder
Upload
Find objects by prefix
1

□	Name	Type	Last modified	Size	Storage class
□	x1-one.txt	txt	February 25, 2021, 01:49:37 (UTC-08:00)	23.0 B	Standard
□	x2-two.txt	txt	February 25, 2021, 01:49:36 (UTC-08:00)	23.0 B	Standard

Also, I accessed the same bucket using AWS CLI S3 command.



```
$ awscli s3 ls  ${PROJECT_BUCKET}  --recursive
2021-02-25 09:40:52          0 image-files/
2021-02-25 09:40:28          0 text-files/
2021-02-25 09:49:37         23 text-files/x1-one.txt
2021-02-25 09:49:36         23 text-files/x2-two.txt
```

Summary

With the VPN connection between laptop and VPN server, I am successfully able to access AWS S3 bucket that is limited to the specific IP address of VPN server.

The AWS S3 Bucket Policy is used to limit S3 access only to VPN server IP address. With VPN connection from laptop, the browser or AWS CLI command from laptop is accessing the AWS S3 bucket.