

ICT & Infra S3 S/NO week 6: AWS VPC Transit Gateway

Date: Sep 2020
Version 1.0

Class:

Student numbers:

Student names:

There was no demo so this is what we did:

| Customer gateways (1/1) Info | | | | | | | Actions | Create customer gateway |
|--|-----------------------|-----------|---------|------------|---------|--|---------|-------------------------|
| Filter customer gateways | | | | | | | | |
| Customer gateway ID: cgw-01f4c64288b3fc194 X Clear filters | | | | | | | | |
| Name | Customer gateway ID | State | BGP ASN | IP address | Type | | | |
| firepass-cgw | cgw-01f4c64288b3fc194 | Available | 65000 | | ipsec.1 | | | |
| cgw-01f4c64288b3fc194 / firepass-cgw | | | | | | | | |

Created Customer Gateway

| Virtual private gateways (1) Info | | | | | | | Actions | Create virtual private gateway |
|---|----------------------------|----------|---------|-----|------------|--|---------|--------------------------------|
| Filter virtual private gateways | | | | | | | | |
| Virtual private gateway ID: vgw-0c77e1557b97b9cda X Clear filters | | | | | | | | |
| Name | Virtual private gateway ID | State | Type | VPC | Amazon ASN | | | |
| firepass-vpg | vgw-0c77e1557b97b9cda | Detached | ipsec.1 | - | 64512 | | | |
| Select a virtual private gateway | | | | | | | | |

Created Virtual Private Gateway

| Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway | Customer gateway ID |
|--------------|-----------------------|-----------|-------------------------|-----------------|-----------------------|---------------------|
| firepass-vpn | vpn-0913f815f8eeb622d | Available | vgw-0c77e1557b97b9cda | - | cgw-01f4c64288b3fc194 | 145.220.0.0/24 |

Created VPN Connection using the vgw and cgw.

Next, I attached the Virtual Private Gateway to our firepass VPC.

```

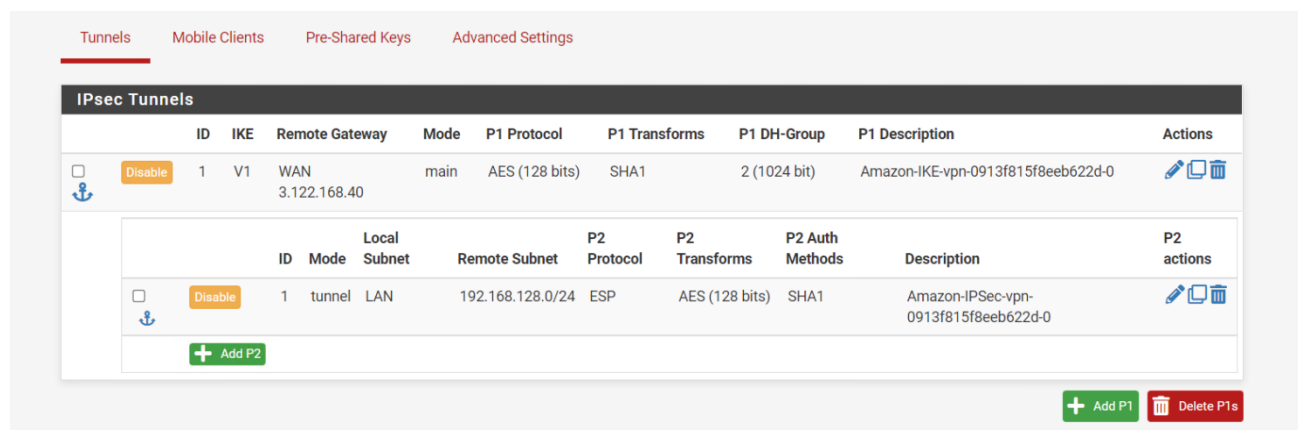
vpn-0913f815f8eeb622d.txt - Notepad
File Edit View

!! Amazon Web Services
!! Virtual Private Cloud

! AWS utilizes unique identifiers to manipulate the configuration of
! a VPN Connection. Each VPN Connection is assigned an identifier and is
! associated with two other identifiers, namely the
! Customer Gateway Identifier and Virtual Private Gateway Identifier.
!
! Your VPN Connection ID      : vpn-0913f815f8eeb622d
! Your Virtual Private Gateway ID : vgw-0c77e1557b97b9cda
! Your Customer Gateway ID     : cgw-01f4c64288b3fc194
!
!
! This configuration consists of two tunnels. Both tunnels must be
! configured on your Customer Gateway for redundancy.
!
! -----
! IPsec Tunnel #1
! -----
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption, authentication, Diffie-Hellman, lifetime,
! and key parameters. The IKE peer is configured with the supported IKE encryption, authentication, Diffie-Hellman
! parameters. Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group
! Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
! You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH
! groups like 2, 14-18, 22, 23, and 24.
! NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify th
!
! Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
! The address of the external interface for your customer gateway must be a static address

```

I downloaded the configuration file to be able to do the configuration in pfSense.



I set up 2 IPsec tunnels using the configuration files.

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|--------------------------|--------|----------|----------|------|-------------|------|---------|-------|----------|------------------------------|---------|
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4 TCP | * | * | * | * | * | none | Allow all traffic from IPsec | |

Add
 Add
 Delete
 Save
 Separator

I created a firewall rule that allows all traffic from IPsec.

I did the same thing in the Security Groups. I allowed all traffic from my pfSense Server.

Routes (3)

Filter routes Both

< 1 >

| Destination | Target | Status | Propagated |
|-----------------|------------------------|----------|------------|
| pl-6ea54007 | vpce-089fc6b4fd2681269 | ✓ Active | No |
| 192.168.0.0/16 | local | ✓ Active | No |
| 192.168.14.0/24 | vgw-0c77e1557b97b9cda | ✓ Active | Yes |

I enabled propagation in the subnet I used.

| Name | VPN ID | State | Virtual private gateway | Transit gateway | Customer gateway | Cust |
|--------------|-----------------------|-------------|-------------------------|-----------------|-----------------------|------|
| firepass-vpn | vpn-0913f815f8eeb622d | ✓ Available | vgw-0c77e1557b97b9cda | - | cgw-01f4c64288b3fc194 | 145. |

vpn-0913f815f8eeb622d / firepass-vpn

Details **Tunnel details** Static routes Tags

Tunnel state

| Tunnel number | Outside IP address | Inside IPv4 CIDR | Inside IPv6 CIDR | Status | Last status change | Details | Certificate ARN |
|---------------|--------------------|-------------------|------------------|--------|---|---------|-----------------|
| Tunnel 1 | 3.122.168.40 | 169.254.26.96/30 | - | ✓ Up | November 27, 2022, 20:02:34 (UTC+01:00) | - | - |
| Tunnel 2 | 3.125.162.228 | 169.254.17.212/30 | - | ✓ Up | November 27, 2022, 20:35:51 (UTC+01:00) | - | - |

► Tunnel 1 options [Info](#)

The VPN is up and running.