strongSwan IPsec IKEv2 server with Windows client authenticating with userid and password

1. Set up VPS, domain name, and DNS

The assumed starting point is that you have a Linux virtual private server (VPS) with 1 gigabyte of RAM running Ubuntu 22.04. You also have your own domain name. Once you have the server and the domain name, create a DNS record type `A` pointing from your server's host name (`moon.cs101.com` in our examples) to the your server's IP address.

2. Set up server

SSH into your server using a terminal emulator or an app such as PuTTY or PowerShell.

```
ssh root@moon.cs101.com
```

Suppress verbose login messages:

```
touch .hushlogin
```

Get your existing package metadata up to date and upgrade all your existing packages:

```
apt update && apt upgrade
```

Protect your server with `iptables`, replacing `<HOME-IP-ADDRESS>` by your actual home IP address. You need to open the firewall for UDP input on ports `500` and `4500`, and also for protocols `AH` and `ESP`. Also "masquerade" the source IP address on outbound packets by setting it equal to the IP address of the server (as opposed to the IP address of the original client). Replace `ens3` by your actual interface name.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -s <HOME-IP-ADDRESS> -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p ah -j ACCEPT
iptables -A INPUT -p esp -j ACCEPT
iptables -A INPUT -p udp --dport 500 -j ACCEPT
iptables -A INPUT -p udp --dport 4500 -j ACCEPT
iptables -P INPUT DROP

iptables -t nat -A POSTROUTING -s 10.0.8.0/24 -o ens3 -j MASQUERADE

ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p ipv6-icmp -j ACCEPT
ip6tables -P INPUT DROP
```

Check that you can still access the server with these rules before you make them permanent:

```
exit
```

```
ssh root@moon.cs101.com
```

On you're sure you can get back in, make the `iptables` rules permanent:

```
apt install iptables-persistent
```

3. Enable forwarding

Create a new configuration file in the `/etc/sysctl.d` directory with a single line in it:

```
echo 'net.ipv4.ip_forward=1' > /etc/sysctl.d/40-ipv4-forward.conf
```

Make this change effective immediately:

```
sysctl -p /etc/sysctl.d/40-ipv4-forward.conf
```

4. Install packages

Install strongSwan and its related packages by entering the command:

```
apt install strongswan libstrongswan strongswan-pki \
    libstrongswan-standard-plugins libstrongswan-extra-plugins \
    strongswan-swanctl strongswan-charon strongswan-starter \
    strongswan-libcharon libcharon-extra-plugins \
    libcharon-extauth-plugins charon-systemd libtss2-tcti-tabrmd0
```

5. Create Certificate Authority

Create a self-signed Certificate Authority (CA) key and certificate as follows.

Generate a private key for the CA:

```
pki --gen --outform pem > /etc/swanctl/private/cs101Key.pem
```

Generate a self-signed CA certificate with a lifetime of 10 years (3652 days). Replace country `CA`, organization `CS101`, and common name `CS101 Root CA` with your own choice of values.

```
pki --self --ca --lifetime 3652 --in /etc/swanctl/private/cs101Key.pem \
    --dn "C=CA, O=CS101, CN=CS101 Root CA" --outform pem \
    > /etc/swanctl/x509ca/cs101Cert.pem
```

6. Create server certificate

Generate a private key for the host `moon.cs101.com`:

```
pki --gen --outform pem > /etc/swanctl/private/moonKey.pem
```

Create a PKCS#10 certificate request that has to be signed by the CA. Notice that both Common Name and Subject Alt Name specify the DNS name of the server.

```
pki --req --type priv --in /etc/swanctl/private/moonKey.pem \
    --dn "C=CA, O=CS101, CN=moon.cs101.com" \
    --san moon.cs101.com --outform pem \
    > /etc/swanctl/x509/moonReq.pem
```

During the period 1998-2000, the Internet Engineering Task Force (IETF) issued versions 00 through 05 of an Internet Draft on Public Key Infrastructure (PKI) Requirements for Internet Protocol (IP) Security. These drafts proposed an extended key usage (EKU) object identifier (OID) of 1.3.6.1.5.5.8.2.2 to mean IPsec Internet Key Exchange (IKE) Intermediate. The construction of the OID was ISO (1), identified organization (3), Department of Defense (6), Internet (1), security (5), mechanism (5), IPsec (8), certificate(2), and IKE Intermediate (2). However, each version of the Internet Draft expired six months after its date of issue. The IKE Intermediate OID never became part of Request for Comments (RFC) number 3280 on Internet X.509 Public Key Infrastructure. Today many certification authorities, including Let's Encrypt, will ignore OID 1.3.6.1.5.5.8.2.2 on certificate signing requests (CSRs). But despite the expiry of the Internet Drafts, Microsoft and certain other companies incorporated the IKE Intermediate OID into their logic for handling IPsec VPNs. Therefore we specify `--flag ikeIntermediate` when we sign the certificate, so that it will be acceptable to Microsoft clients.

```
pki --issue --cacert /etc/swanctl/x509ca/cs101Cert.pem \
    --cakey /etc/swanctl/private/cs101Key.pem --type pkcs10 \
    --in /etc/swanctl/x509/moonReq.pem --flag serverAuth \
    --flag ikeIntermediate --lifetime 365 --outform pem \
    > /etc/swanctl/x509/moonCert.pem
```

7. Generate client password

Generate a random password for the client named `carol`:

```
< /dev/urandom tr -dc _A-Z-a-z-0-9 | head -c16 && echo ''
```

Example of output from the above command:

```
iM0AeDaVmc9FIWRz
```

8. Configure strongSwan server

Create a new file for IKEv2 connections with userid and password authentication:

```
vi /etc/swanctl/swanctl.conf
```

Delete the template and insert a new configuration based on the example below:

```
connections {
  rw-eap {
    version = 2
    proposals = aes192gcm16-aes128gcm16-prfsha256-ecp256-ecp521,aes192-sha256-
modp3072,aes256-sha256-modp2048,aes128-sha256-modp2048,aes256-sha1-
modp2048,aes128-sha1-modp2048
    rekey_time = 0s
    pools = primary-pool-ipv4
    fragmentation = yes
    dpd_delay = 30s
    send_cert = always
    local {
      certs = moonCert.pem
      id = moon.cs101.com
    }
    remote {
      auth = eap-mschapv2
      eap_id = %any
    }
    children {
      ikev2-pubkey-child {
        local_ts = 0.0.0.0/0
        rekey_time = 0s
        esp_proposals = aes192gcm16-aes128gcm16-prfsha256-ecp256-
modp3072,aes192-sha256-ecp256-modp3072,aes256-sha256-modp2048,aes128-sha256-
modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048
      }
    }
  }
}
pools {
  primary-pool-ipv4 {
    addrs = 10.0.8.0/24
    dns = 8.8.8.8,8.8.4.4
  }
}
secrets {
   eap-carol {
      id = carol
      secret = iM0AeDaVmc9FIWRz
   }
}
```

Save the file `/etc/swanctl/swanctl.conf`.

9. Restart strongSwan

Restart strongSwan with your new configuration:

```
systemctl restart strongswan-swanctl
```

Check that strongSwan is `active (running)`:

```
systemctl status strongswan-swanctl
```

Your server work is done for now, so exit from the SSH session with the server:

```
exit
```

10. Edit Registry on Windows IKEv2 client

Windows is limited to MODP1024 (Diffie-Hellman Group 2), which can prevent matching policies with the server if you do not configure your server to allow for this limitation.

Use the Registry Editor to allow the use of MODP2048.

1. Press the **Win**+**r** keys, type `regedit`, then press **Enter**.
2. If Windows asks you if you want to allow the Registry Editor to make changes to your device, click **Yes**.
3. In the tree in the left pane, navigate to `HKEY_LOCAL_MACHINE` > `SYSTEM` > `CurrentControlSet` > `Services` > `RasMan` > `Parameters`.
4. Right-click on `Parameters`, and insert a new DWORD (32-bit value).
5. Set the name of the new key-value pair to `NegotiateDH2048_AES256`.
6. Set the value to `1`, which means allow the use of AES-256-CBC and MODP2048.
7. Close the Registry Editor.

11. Copy CA certificate to Windows IKEv2 client

Copy the CA certificate `.pem` file to your Windows workstation. This copy does not need to be secure, but you still, for example, use the secure copy (`scp`) command in PowerShell:

```
scp root@moon.cs101.com:/etc/swanctl/x509ca/cs101Cert.pem
Downloads/cs101Cert.pem
```

12. Install CA certificate on Windows IKEv2 client

1. Open the **Settings** app.
2. In the search box, type `certificates`.
3. Open the selection **Manage computer certificates**.

4. If necessary, allow the app to make changes to your device by clicking **Yes**.
5. Select the menu item **Action** > **All Tasks** > **Import**.
6. Click **Next**.
7. Browse to the file `Downloads\cs101Cert.pem` and click **Open**.
8. Click **Next**.
9. Select **Trusted Root Certification Authorities**.
10. Click **Next**.
11. Click **Finish**.
12. Click **OK**.

Close any **Settings** windows that are open.

13. Add the new VPN connection

Use **Settings** > **Network & Internet** > **VPN**.

Click the plus sign for **Add a VPN connection**.

1. Set the VPN provider to **Windows (built-in)**.
2. Set the connection name to (for example) `moon`.
3. The server name or address in our example is `moon.cs101.com`.
4. The VPN type is **IKEv2**.
5. The type of sign-in info is **User name and password**.
6. Our example user name is `carol`.
7. Our example password is `iM0AeDaVmc9FIWRz`.
8. Check the box for **Remember my sign-in info**.

9. Click **Save**.

14. Connect IKEv2 client to IKEv2 server

Now connect your client to your server.

Still in **Settings** > **Network & Internet** > **VPN**, select your VPN `moon`.

Click Connect.