Physical MIP Red Hat Connection to PCTE Event

Physical MIP Connection to PCTE Via Global Protect and OpenVPN

Installable packages provided come from the DIP reposync server that is PMO provided

RHEL 8 OS (MIP) is required. MIP build v3.5 or v3.7

United States Government CAC required

You must have an active PCTE account

You will need a completed 2875 for a pcte.texnet1.net account. See PCTE Confluence for 2875 template

You will need an active internet connection

*****PCTE Physical MIP Connection Wiki (CAC Authentication)**

1. **Download a 2875 access request form and submit**
    a. Download a 2875 form from here: pcte_texnet1_net_2875_template.pdf
    b. Sign and submit form to jeff.mccarty.1.ctr@us.af.mil and Cc mahlon.rivas.ctr@us.af.mil
2. **Fix BIOS Settings** (Only if MIP is not booting correctly. Optional)
    a. Boot MIP hitting F2 key to get into BIOS
    b. Click Load Defaults at the bottom and select BIOS Defaults option. Then click OK to proceed to reboot
    c. Click F2 key to get back into BIOS
    d. Got to Storage and for SATA settings change "Raid-On" to "AHCI/NVMe"
    e. Save settings and reboot to proceed.
3. **Login to the MIP**
4. **Install DoD certificates for pcte.texnet1.net**
    a. For access to pcte.texnet1.net, the following certs are needed:
        i. DoD Root CA 3
        ii. DOD SW CA-60
        iii. Your CAC certificate's issuing CA certificate
            1. To find this, go to your CAC Authentication Certificate's properties
            2. Under the General tab, the certificate will be listed in the "Issued By" field. Take this down because it will need to be imported as well.
    b. All DoD certs can be downloaded at the following link:
        i. AllDoDCerts.zip
        ii. Extract certificates to any folder
    c. Firefox browser must be used to connect to pcte.texnet1.net. Import the certs in Firefox:
        1. In Firefox, got to Preferences > Privacy and Security > SCROLL DOWN > View Certificates. Enter CAC PIN if prompted. (Master Password is CAC PIN)
        2. Go to Authorities. Select the Import button and select the appropriate certificates mentioned earlier**. If prompted for the type of trusts, select all checkboxes and click ok**
5. **Make sure Firefox is set as default browser**
    a. In Firefox, go to Preferences > General
    b. Select "Make Default" to make Firefox the default browser if it is not already selected.
6. **Test OWA to make sure CAC works appropriately (Optional)**
    a. In Firefox, browse to https://webmail.apps.mil. Enter PIN and select appropriate certificate.
7. **Install Global Protect (GP) VPN client**
    a. The GP Client for Red Hat and dependencies can be found in a zip file at the 318 RANS Range Support Team space on PCTE Confluence (Scroll to bottom) (https://rcs00-wiki.pcte.mil/display/318RANS/Physical+MIP+Connection+to+PCTE).
    b. Download the redhat8_gp_5.2.5_with_Deps.zip package here: redhat8_gp_5.2.5_with_Deps.zip. Extract the contents to a folder using unzip. Ex: unzip redhat_gp_5.2.5_with_Deps.zip -d <*destination*>
    c. If you run into issues where it is skipping files during extraction, run 7za x <*zip file name*> instead
    d. Make sure you are in the folder you extracted to and run the following:
        i. yum --disablerepo=* --nogpgcheck localinstall ./*.rpm
        ii. Select y to accept any install prompts for installation
    e. Global Protect should install and the agent GUI may pop up. Ignore the pop up for now and continue set up.
8. **Enable Global Protect to use your default browser (Firefox)**
    a. Open /opt/paloaltonetworks/globalprotect/pangps.xml with a text editor
    b. In the Settings area, between <default-browser> and </default-browser> add yes. You may need to add the default-browser tags.
    c. Example: <default-browser>yes</default-browser>
    d. If regioncode tag is not showing, it is ok to proceed. See example below.
        i. gp_gps_xml.jpg
        ii. Save the changes to the file and exit
9. **Copy DoD Root CA 3 and DOD SW CA-60 to Global Protect Directory**
    a. From the certs you downloaded earlier:
    b. Rename DoDRoot3.cer to DoDRoot3.pem
    c. Rename DOD SW CA-60.cer to DOD SW CA-60.pem
    d. Move/Copy the pem files to /etc/pki/ca-trust/source/anchors/
    e. Run "update-ca-trust"
    f. Reboot computer.
10. **Clear out any .dat files if any (May not be required, but resolves frozen sessions if any)**
    a. cd /home/<*usename here*>/.GlobalProtect
    b. rm ./*.dat
11. **Connect to pcte.texnet1.net via the Global Protect client (***This may take a bit. You may see several tabs open in Firefox before the Global Protect icon shows connected.***)**

a. After logging back on, In the top right of the desktop there should be a globe icon. Click it to open the Global Protect client GUI (If not already open).
b. Make sure you can resolve with the command: nslookup pcte.texnet1.net
c. In the box where it is requesting a portal, type in pcte.texnet1.net, click Connect
d. When prompted for PIN, enter CAC PIN and select the appropriate certificate (non-email cert (PIV)). You may be prompted more than once.
e. Make sure your browser pops up and shows Authentication Complete on the page and that the Global Protect icon (Top Right) shows connected and not a red dot.
f. If you are prompted to open links with Global Protect, click the check box to remember and select Open. This will prevent any of these pop ups in the future when connecting.

12. **Ping Check**
    a. Reach out to the 318 Simulator Support Cell Slack for the IP address of the Event you will be connecting to or reference here
    b. Make sure you can ping that IP
13. **Download OpenVPN certificate for access to DIP/MPNET network for AFNET Scenario1**
    a. Browse to https://192.168.3X.XX and login (assessor | Simspace1!Simspace1!) (IP address from Step 12)
    b. Go to VPN OpenVPN --> Client Export
    c. In the first field labeled "Remote Access Server", make sure the appropriate server for RHEL is selected.
    d. Scroll down to the certificates to download.
    e. For RHEL, select “Most Clients” button to download.
14. **Establish OpenVPN connection**
    a. RHEL
        i. Open the terminal and go to the directory of the certificate that was downloaded. Run openvpn <*certificate name here*>.
        ii. Make sure “peer initiation initialized” appears.
        iii. Ping 192.168.100.1. This is the VPN interface on the Pfsense in the DIP.
        iv. Open /etc/resolv.conf
            1. Comment out any existing nameserver entries and add "nameserver 192.168.100.1" to the file. Save and exit.
15. **Test Connection to Range**
    a. Controller: ping 10.101.35.15
    b. Browse to https://dip.controller.lan and login.
    c. ping Mission Partner DC
    d. ping 8.8.8.8 (DNS on simulated Internet in PCTE)
    e. If any of these are unsuccessful, please let 318 RANS support know.
16. **You should now be connected to the range with your MIP**

******You can disable Global Protect from the Global Protect icon dropdown menu when not in use**

******When done using Global Protect VPN, be sure to restart the network service or disable and re-enable your NIC/Adapter to reset settings to original**

Attachments: 1. pcte_texnet1_net_2875_template.pdf
2. redhat8_gp_5.2.5_with_Deps.zip