Current DMZ Firewall Process

To request a change to the DMZ Firewall:

- Go to https://servicecenter.oit.ucdenver.edu/CherwellPortal/
- Click login
- Select make a request
- Select security services, Firewall/IPS
- Select Firewall Request
- Complete the form to submit a DMZ Firewall request

Helpful tips:

- If the server is requesting access to or from internet/affiliates or is a webserver, it will need a public IP address: 140.226.x.x or 132.194.x.x. The server location will determine what DMZ IP address is assigned.
- If the server is a virtual machine, the Computing Infrastructure (CI) team can assist with giving it a new public IP address.
- If the server is a physical host, the Network Core team can help provide a public IP address and place server on appropriate VLAN. This will be done via a task through Cherwell or separate email that SecOps will generate.
- If the server is, for example, example.ucdenver.PVT, the owner will need to get a public domain name such as: example.ucdenver.EDU. Following are the steps to initiate that request:
  1. Pick your preferred computer name and join the computer to the domain using ucdenver.pvt. (The CI team will fix the name with DNS)
  2. Request the appropriate 3rd level and 4th level domain names using the link here (you will need to be connected to the VPN to access the site)
     https://my.ucdenver.edu/services/technologysupport/services/services/pubweb/Pages/UrlRedirectRequest.aspx
     a. A 3rd level domain name such as pathology.cuanschutz.edu is approved by our CIO and this process is tightly controlled.
     b. A 4th level domain name such as copathct.pathology.cuanschutz.edu is approved by our web services director and is an easier process.
- Make sure the server has a public static IP address and work with the security team to get the firewall exemption. (140.226.x.x or 132.194.x.x)
- Request the public certificate type “Comodo Unified Communications Certificate” when enrolling your server’s CSR at https://hard.cert-manager.com/customer/ucdenver/ssl
- When you have the firewall and the domain approved, the CI team can point the approved domain names to your server. (This step will be done via a task through Cherwell or separate email.)

Please note the new DMZ security controls coming.

The system will need:

- To be on Domain and on an application patching program.
- Antivirus protection
- A personal firewall (Windows/ Linux preconfigured by CI)
- Wazah (Ossec) – which can be obtained from the Security Operations team