Changes in Brown's Network Security Zones

Stephanie Obodda - 2024-11-21 - Comments (0) - Wired Connection

As part of an initiative to secure network devices at Brown, two significant changes are being made that may impact how you use the wired ethernet network. This change will affect departmental buildings and offices used by faculty and staff. We are providing this article for departmental computing staff to help identify which users in their department might be affected.

Private addresses will be used instead of the previous internet routed IP addresses that begin with 128.148 or 138.16. The new IP addresses begin with 10. The second change is the use of dynamically allocated IP addresses. Also known as DHCP, the dynamic allocation means you may not always get the same IP address when you connect. The questions below may help you decide if you need a reserved DHCP address so that you do get the same IP address when you connect.

Do you need to remotely access your workstation (SSH, RDP)? Do you access other devices on the network? (Network attached storage, printer, or lab equipment)?

If yes, using a DNS name instead of the IP address will make network changes easier. Don't know the DNS name of a device? We can help you make sure one is assigned. If the device uses DHCP, it can be configured to automatically update DNS if the IP address changes, so you never have to know what the IP address is and the name will never change.

If dynamic DNS is not an option, then, you'll need to request a reserved IP address. If you don't, and later decide you do want to remotely access your workstation or device, your IP address will need to be changed to a reserved IP address. Your department computing support person can submit a request on your behalf through a Remedy Incident ticket or they may have access to make this change themselves.

The new security zone networks use private IP address space which means you cannot directly access workstations or devices from the Internet. You will need to use the VPN, or Virtual Private Network. Article: How to use Brown's VPN

Do you access resources on the Internet that are limited to specific source IP addresses?

If so, you will need to provide the PAT/NAT address or range of addresses that are used for Internet access. Please contact the Service Desk to find out what to use. This should be

provided to the Internet resource so they can add that to their allowed list before you are moved into the network security zone.

Do you have devices or servers that need to be accessed from the Internet?
If yes, there is a separate security zone for this called the DDMZ. Servers or devices that are placed in the DDMZ are subject to strict security policies that require frequent patching and vulnerability scans that are done regularly by CIS. Before the device or server is moved into the DDMZ, you will need to determine which firewall ports need to be opened. By default, no access is allowed to devices or servers in the DDMZ. If you are unsure what ports are needed, please open a ticket with the Service Desk.

Best practice dictates that workstations and desktops should not be placed in the DDMZ.