Network Traffic and SSH Login Blocking

If you are having trouble logging into a system or getting access to a service on the SoIC systems, this page may help you determine the cause of the problem. Your connection may be getting blocked for some reason and this page describes the common blocks you may encounter.

1. **SSH Login Blocking** - Many of the SoIC Linux systems allow SSH connections from anywhere but they block IP addresses that have had too many failed login attempts. This is necessary to prevent ssh login bots from causing problems like getting ADS accounts locked out. You can use the SSH Block Checker to see if your IP addresses is blocked. If you do get blocked, you can always circumvent the block by making a connection to the IU VPN. A common error message to receive if you are blocked in this way is:

```
ssh_exchange_identification: read: Connection reset by peer
```

2. **Operating System Firewalls** - As is common for most systems, SoIC systems will almost certainly have a local OS firewall in place to either block all traffic to certain ports or to limit access to ports to certain IP addresses or networks. For example, on the SoIC linux systems you may find that you have access to ports from the local subnet but not from IP addresses outside of our local networks. Or, you are likely to find many ports blocked outright.

3. **Border Router Blocks** - The border routers at IU (and managed by UITS) also have blocks implemented for a limited number of service-specific ports. For example, Windows SMB and Remote Desktop services are blocked from outside IU as is MySQL. To access these blocked services from outside IU you will first need to make a connection to the IU VPN.

4. **Rogue System Blocks** - UITS does network monitoring to try and identify systems that are compromised or otherwise exhibiting some type of rogue behavior (such as port scanning). When they identify a rogue system they will either block that IP address and/or prevent that system from getting an IP address via DHCP. In either case, the target system will be unable to access network services, both on campus and off. You can use the UITS Block Lookup Page to see if any of your systems have been blocked.

5. **DNS Filtering** - IU is doing DNS filtering which means that if you do a DNS lookup of a known rogue system, the IU DNS servers will return the IP address of a DNS sinkhole page instead of that of the rogue system. In most cases, this is a good thing and helps protect your systems from compromise. However, if you are doing security-related research that involves contacting known rogue sites you may want to ensure that you are using a DNS server that does not do this type of filtering, such as the Google Public DNS or OpenDNS. Please see the IU KB page At IU, what is the DNS filtering service? for further details about this service. If you need help configuring a system to use an alternate DNS server, please contact us.

If you have any questions about these issues as they pertain to the systems in the School of Informatics and Computing, please contact us. If you have questions that are related to IU but not the School of Informatics and Computing, please contact the UITS Support Center.