University Security

One of our primary needs is to ensure the absolute security of all UB designated production networks. This page should list out the provisions we have to ensure no traffic leakage.

Traffic Rules

Our firewall rules page has detailed information regarding specific rules, as well as the “idea” behind them. A high level overview is that we block all publicly announced UB IP Ranges (announced by AS3685), and whitelist only specific subnets / IPs that are required to operate. As we route all our internal traffic going out to the internet through our firewall, we can ensure there is no traffic leakage.

Dual-Homed Machines

We aim to have a very limited amount of dual-homed machines, which are machines that have interfaces for both the CSE Uplink and Red Team Network. We have divided our dual-homed machines into two separate categories.

Web Server

Our public webserver (the server that hosts ubnetdef.org, and all subdomains) is a dual-homed machine. The main reason this machine is dual-homed is so that it can proxy some requests to some of our internal machines. These proxy requests are a one-way connection.

To ensure the security of this server, we have placed additional firewall rules on this machine. More details on this machine can be found on this page.

Jump Boxes

We also operate a Windows Server 2012 RDP Jump Box. This server is behind the CSE Production firewall, limiting access from non-UB IP ranges.

More details on this machine can be found on this page.

MGS 650 bastion

`cdr-netscan` is a Debian VM used by MGS 650. These students are not given access to vCenter, so they connect to this machine via SSH. This machine is connected to the Cloud network.

User Accounts

We currently have vCenter joined to UB's Active Directory, reducing the needs for additional accounts for the majority of UBNetDef.

To handle our internal infrastructure management (storage servers, routers, monitoring), we have an additional centralized authentication server. This machine is only accessible while on our internal networks.