LUKE DUNK
7/24/2024
PROF. DUVALL

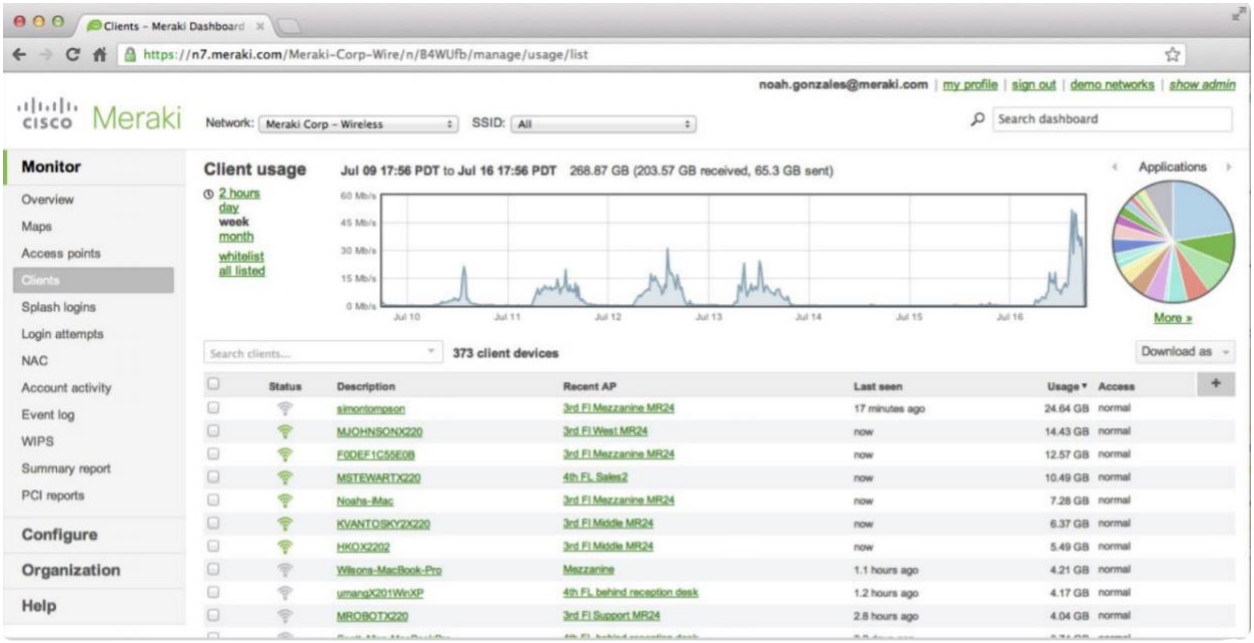
Journal Entry #6

Today marks my final 300 hours at Atlantic Bay Mortgage Group as their Information Technology Intern working alongside their network administrators. To pick up from my last journal entry, I completed my mini port labeling project that required me to label each device at each branch. The overall goal is to implement 802.1x port-based authentication using EAP-TLS to secure our internal network. Using a RADIUS server, users are authenticated to our internal network through their Active Directory account information. This ensures that bad faith actors cannot just walk into a branch location and plug-in an ethernet cord right into our network. In addition, Atlantic Bay utilizes RADIUS for wireless authentication for Wi-Fi access. For example, a mortgage banker may want to connect their iPhone to our Wi-Fi while they are in-office. In this case, we hardcore the device's MAC addresses and a unique shared secret key to our RADIUS server. Therefore, this unique password only works with that device and cannot be shared. Not only that, but we also segment these devices inside a separate VLAN, we refer to as the 'GuestNet', to separate them from our critical VLANs. Since many of our devices do not have an AD object entry (printers, phones, etc.) my project allowed the team to create special entries for these unique devices using their MAC address and the specific port they operate on.

Atlantic Bay has a very complex networking environment, and still, I don't fully understand how everything works. However, I have a broad understanding. On-premises, we focus on hosting our internal banking applications and failover / disaster recovery technologies for our operations. In the cloud, we focus on remote connectivity with VPN concentrators for our users and focus on hosting cloud-based applications. In addition, we host more failover / disaster recovery applications in these cloud systems. In both environments, we host most of the same technologies. If the cloud environments go offline, we have the capability to replicate our infrastructure to our on-premises servers. If our headquarters goes offline, we could move our internal applications to the cloud and restore our on-premises operations from cloud backups. No matter if it's in AWS, Azure, or on-site, there are failover technologies on every end to keep operations running no matter what. Unfortunately, I cannot provide any actual reference pictures of our network environment, as Atlantic Bay does not want this information public. In more recent journal entries, I had to get my supervisor to read through my entries to ensure I don't reveal too much of their infrastructure. However, I can briefly provide screenshots of the systems I use to complete my objectives while on their team.

LUKE DUNK
7/24/2024
PROF. DUVALL

Since our environment uses Cisco products, we utilize their SD-WAN application called Meraki to control each device within every branch. This allows us to quickly deploy products using pre-defined templates and easy configurations depending on our need. Just this week, I installed a new Access Point inside our office and used Meraki to claim our new product, apply our pre-defined template, and configure our AP to our specific needs.



For monitoring our sensors, on-premises networks, and our cloud environments, we use a software application called PRTG. This gives us warnings and alerts to our team about our infrastructure and potential problems. PRTG is like what a SIEM does. PRTG collects information from different sources, stores logs, and alerts on potential problems. Just like how a SIEM collects logs and alerts on events or cyber incidents.