Network services for Raspberry Pi’s

Name: NetBeez

Purpose: NetBeez allows you to monitor your network infrastructure from remote locations. It offers real-time network activity not just for the central or core infrastructure but even end-users statistics as well. Unlike other traditional tools that only tells you an error after it has occurred, this application uses predictive AI to generate reports of problems that could arise in the future. It offers many other services such as DNS, VPN, ICMP and FTP to name a few. All these are key features to maintain and update a network infrastructure as the company grows and expands.

Importance: NetBeez is especially helpful and works perfect for our network environment due to being a fully remote network engineering team. Unlike traditional networking tools where you have to be at a certain location to monitor the network, NetBeez offers a VPN service where anybody can access it and troubleshoot from anywhere. This tool integrates perfectly with almost any type of API which allows seamless integration for any network infrastructure out there. It also works hand to hand with Raspberry Pi’s because they are a lightweight tool that don’t require a lot of resources. Since Raspberry Pi’s are not that expensive compared to other services or networking tools that require hefty money, we can easily deploy them anywhere that is needed and save money.

Name: Suricata

Purpose: Suricata is a IDS/IPS tool that allows for network traffic analysis to detect malware, deep packet inspections, and even offers signature-based or anomaly-based detection. Not only does it work for HTTPS/HTTP traffic only but also works for other protocols in various layers such as TCP, UDP, ICMP, SSH, and many more. Suricata also allows for specific parameters in the customization panel so you can tailor it to whatever the network needs. Exporting is super easy because you can format to almost any file type whether that would be JSON, EVE JSON, or even PCAP.

Importance: Suricata would do well in our network environment because as a network engineer not only is it important to maintain and monitor our network infrastructure but to make sure it is protected at all times. Since we are heavy on remote work, connections are going to be coming in and out all day. The last thing we want as a team is to allow unwanted connections into our infrastructure. This is an open source tool as well which adds flexibility like integrating it with our other application NetBeez to have multiple applications working as one.

Name: OpenWRT

Purpose: OpenWRT allows you to modify QoS policies on a network infrastructure. Quality of services plays a key role in networking because it allows fine-tuning specific traffic to have more bandwidth than other types of traffic. This is especially helpful in an environment where you have multiple types of traffic coming in and out such as VoIP, video conference calls, HTTP traffic or even ICMP traffic. OpenWRT allows for specific percentages or total bandwidth for every application

Importance: OpenWRT is a key essential for an enterprise network because since you are dealing with multiple types of traffic from such a large network, you need to proportionate it according to what is more important to least important. Things such as VoIP and video conference calls should be a top priority in every company's list but things such as ICMP should not be taking up half of the bandwidth.

Name: Pi-Hole

Purpose: Pi-hole is a universal network ad-blocker that blocks advertisements and unwanted domains to all your systems, also known as a DNS Sinkhole. This results in enhancing network security, privacy, and performance by eliminating unwanted traffic. How it works is simple: whenever a DNS inquiry is made, Pi-Hole goes into the DNS database and sees if it is part of a ad or tracker domains and if it is, it simply returns a null address so ads can’t load on the webpage but allows the real webpage request to load.

Importance: Pi-Hole is essential in an enterprise network because you want to minimize all traffic to ensure the best network performance. Not only performance but you want to protect your network and end-users from malicious ads and domains because you can have the best network security but if your end-users aren’t protected then your network is at risk. It is the best of both worlds but also adds that extra layer of privacy so employee information isn't at risk for any phishing attempts.