Uplevel Systems 2.0 FAQ

Why did my performance decrease?

When enabling the IPS IDS firewall the performance and overall bandwidth of the network is subject to the processing rate of the firewall. The processor is rated at 30Mbps however this varies based on the type and quantity of the traffic. Traffic that is encrypted will receive a higher performance rate as compared to unencrypted traffic. For customers having an initial bandwidth of less than 30Mbps they will not experience any change in performance.

Why is the pinging taking longer than normal?

This is completely normal! Because it is done remotely and through the cloud it can take longer for the pings (and their responses) to reach the cloud and then back down. This is to be expected and is not any cause of alarm. Once the ping has returned it with provide the number of packets and delivery time. Please note, as usual, any Firewall rules or idle machines may generate a no response ping to an otherwise healthy machine.

What is the difference between the devices log and network scanning?

The devices view is a passive scan. It only registers devices as online vs. offline when they are communicating with the gateway for example for an IP address. This is a great way to see things are currently communicating with the gateway. The network scan differs by being an active scan. It probes all possible IP addresses in the network for a response giving it the ability to discover devices that are not currently or previously communicating with the gateway.

How do I know what if the IDS alert is malicious or not?

Uplevel's IPS/IDS firewall uses linux-based snort. The rules number is found in the lower left hand corner of the alert and can be googled to find an exact description of the activity being alerted on.