QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Fundamental Filtering of IPv6 Network Traffic

This paper begins a series of IPv6 TIPs to assist network defenders with the security implications of IPv6 deployment. This document will not duplicate existing published documentation concerning the theoretical aspects of IPv6-based network security, but will focus more on the first steps of a "HowTo" for network defenders.

You will find non-vendor-specific provisioning of IPv6-based network traffic filtering via basic types of traffic blocking suggestions, identification of deprecated addresses, a brief discussion on ICMPv6, tunneling, and additional topics to consider when developing an IPv6 implementation strategy.

Implementing IPv6 introduces a myriad of challenges, including providing security at network borders as well as internal controls. By design, IPv6 enables each host's direct connection to the internet with a completely routable address.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- FilteringIPV6NetworkTraffic.pdf