

Requirements for IPv6 Enterprise Firewalls

(draft-gont-opsec-ipv6-firewall-reqs)

Fernando Gont
Marco Ermini
Will Liu

IETF 95
Buenos Aires, Argentina. April 3-8, 2016

Introduction

- It is rather difficult to infer what are reasonable features to expect in an IPv6 firewall
 - Less confidence with the protocols
 - Less operational experience
- Many operators have to resort to writing (probably suboptimal) RFPs from scratch
- We are trying to fill in that gap
- For instance, this document is derived from one of such RFPs

How the document is organized

- Different categories for the requirements:
 - General Security Features
 - IPv6-Specific Features
 - VPN Security Requirements
 - Denial of Service (DoS) Protection
 - Application Layer Firewall
 - Logging, Auditing and Security Operation Centre (SOC) requirements
 - Console and Events Visualization requirements
 - Reporting requirements

Requirements

- The document aims to mark different each of the requirements/features as:
 - mandatory
 - recommended
 - optional
- ..in the hopes of defining some baseline functionality.

Feedback received so far

- Should clearly state which of the requirements are for stateful vs. stateless firewalls
 - such that e.g. a stateful requirement does not preclude stateless firewalls
- Should move the TCP, UDP, and IPv6 low level details into a separate document
 - then this document can reference such documents
- More consistent use of defined terminology
 - e.g. “communication instance” vs. “session”

Feedback received so far (II)

- This document can specify the type of data that should be offered to the user, but not the User Interface.

Comments?