

1460 - Security

Introduction

Newport's *Revenue, Core & Nodal Protection* (RCNP) security package has been designed to provide security for SIP voice and multimedia services. RCNP prevents service fraud and protects network operators against attacks on core network elements, such as Softswitches or SIP proxies; and of course provides complete security for the Newport 1460 itself.

Newport's RCNP suite addresses security in 3 key areas:

- ♦ Revenue Protection
- ♦ Core Network Protection
- ♦ Node Protection

Revenue Protection

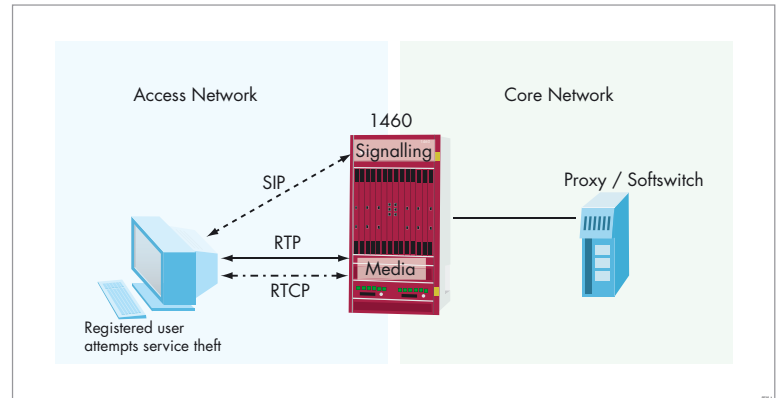
Newport's 1460 session border controller prevents service fraud by policing calls to ensure that subscribers cannot use more bandwidth than they have negotiated.

Policing occurs in both media (RTP) and Real Time Control Protocol (RTCP) streams to prevent rogue users sending information through the RTCP stream undetected while paying only for use of the media stream. Signalling is policed on a per-user basis to ensure that data is not exchanged between users prior to call setup.

Core Network Protection

Newport Networks' Core Network Protection adds critical security policies that prevent Denial of Service (DoS) attacks from impacting core network equipment such as Softswitches. The 1460 provides complete topology hiding for the network, ensuring that the overall topology is not exposed to attacks while also securing privacy of the subscriber base.

In keeping with a forward-looking, IMS-ready strategy, traffic directed at the 1460 can be separated into signalling and media. Media traffic is checked to ensure that it has come from a valid registered user and bandwidth policed so as not to exceed negotiated rates. Media coming from invalid sources is dropped at wire-speed. Signalling traffic is filtered according to user registration. For those registered, signalling is rate-limited on a per-session basis to ensure that neither equipment malfunctions nor fraud attempts generate excessive messages. Traffic from non-registered users is similarly rate-limited to prevent its arrival rate from impacting Softswitches in core networks.



Node Protection

Newport Networks' Node Protection shields the 1460 from malicious Denial of Service attacks. The 1460's unique carrier-class design incorporates physically separate management and data planes so that DoS attacks cannot disrupt management data. Management interfaces are encrypted and kept physically separate from traffic interfaces, with access lists and encrypted passwords used to deny unauthorized access.

The RCNP security suite is provided from the Newport Networks carrier grade platform ensuring that security attacks which occur at maximum line rate and minimum packet size can be dealt with at line rate whilst protecting key network resources and revenues.