

SECURITY and MEDUSA

Date March 2005

Version V3.0 release 170 above

Author TF

Overview

This document relates Internet Security and Phoenix Broadband's Medusa V3 Shared Internet Access product.

Medusa Description

Medusa is a Linux based multi-armed firewall and router with traffic management and billing facilities. It operates by providing shared access for licensees in a business centre and combining their traffic into one or more Internet circuits.

Traffic flows over Ethernet interfaces allocated one per licensee, and for WAN ports. Traffic is routed by rules written from the database. Licensees are allocated their own local IP class C address range including their own gateway.

A User Interface is provided which allows non-technical operators to set up predefined changes to the routing database at a very high level.

Medusa Design

On the general WAN IP, only 2 specific tcp ports are open and available to the public Internet, relating to email. No inbound traffic on any IP address in the range supported by Medusa is otherwise accepted without either a rule or a Nat-originated session.

Remote administration and management is available only to authorised individuals based on a combination of protocol and originating address, plus passwords, and where appropriate, certificates.

The only other traffic accepted inbound by Medusa are Public IP addresses. These are allocated, on request, to individual licensees and are handled either by specific port forwarding rules or as VPN subnets.

Traffic between licensees is prohibited. No physical layer connection between licensees exist as licensees are connected on separate Ethernet ports. Medusa ports only handle IP routing, and IP routing between ports is prohibited - only forwarding to the public gateway is allowed.

Security Principles

Phoenix Broadband follows Cert advisories on Internet related security issues, where relevant.

All Medusas are covered by a Service Level Agreement and are patched according to recommended practice against known vulnerabilities.

Updates, which are issued by RPM, can only be introduced via an authentication process.

Medusa security design generally follows recommended Cert practice, including checksums on disk contents, restrictions on services, limited changes permitted, alerts on unexpected conditions.

All Medusas are remotely monitored around 100 times per day. Activity is logged and logs rotated offsite. SNMP monitoring produces 5 minute bandwidth usage for all ports.

Security Responsibilities

Phoenix Broadband undertakes to maintain the system according to the good practice principles outlined above.

The Business Centre Operator undertakes to physically secure the system against intruders and to maintain an appropriate environment. The operator also maintains a Right-to-Use licence with the Licensee that they will limit use to the guidelines of an agreed Acceptable Use Policy.

The Licensee is responsible for assessing and implementing the appropriate level of security according to their application and business. Where doubt exists, the Licensee should procure an additional firewall or other protection device.

Further Reading

Visit the website www.medusabusiness.com for additional information, specifications etc.

Security practice, www.cert.org