Avenida de la Albufera, 323, pl. 2, of. 13
28031 Madrid (Spain)
Phone: +34 91 803 9251
E-mail:wirelessmundi@wirelessmundi.com

Web:http://www.wirelessmundi.com

COMMS MUNDI IP SECURITY:

Tech sheet

Date: May 2022
Made by: Wireless World

Index

1. INTRODUCTION 3
2 COMPONENTS 3
2.1 firewall 3
2.2 IDS/IPS 3
2.3 Anti virus 3
2.4 Anti Spam 3
2.5 Certificate Authority 3
2.6 IPSEC VPNs 4

1 INTRODUCTION

This document details the technical specifications of the Comms Mundi (CMH) IP Security module product.

2 COMPONENTS

The IP security module is made up of the following components.

2.1 firewall

This component is responsible for allowing or denying IP traffic. The rules can be applied according to the OSI model identifying the traffic from layer 2 (link) to layer 7 (application). Allows you to create rules taking into account the status of the connection.

2.2 IDS / IPS

This component allows traffic to be analyzed in real time, identifying the traffic through the emergency thread rules. If the rule is configured in this way, the traffic identified by the rule is automatically blocked.

2.3 anti virus

This component allows the detection and protection of virus threats by adding more security to email and web proxy services.
The virus database can be updated manually or automatically.

2.4 anti spam

This component allows the detection of Spam in the email service. The detection algorithms are updated with the update system and improve the automatic detection using statistical analysis from emails identified as SPAM or HAM.

2.5 Certificate Authority

This component allows the creation of an own entity for the signing of ssl certificates or for the creation of new orders. Certificates can be used in services that require ssl encryption (sip tls, web portal, vpn users).

2.6 IPSEC-VPN

This component allows the creation of IPSEC VPN encrypted tunnels, you can establish a fixed connection of type: host-to-host, host-to-subnet, subnet-to-subnet, or dynamic tunnels with user authentication either by IKEv1 XAUTH or L2TP.
To use tunnels with user authentication, it is necessary to activate the authentication module.