Universidade de Aveiro
Departamento de Electrónica, Telecomunicações e Informática,
2023

Vasco Regal Sousa

Multiple Client Wireguard Based Private and Secure Overlay Network

DOCUMENTO PROVISÓRIO

"Observation is a dying art."

— Stanley Kubrick

o júri / the jury

presidente / president

ABC
Professor Catedrático da Universidade de Aveiro (por delegação da Reitora da Universidade de Aveiro)

vogais / examiners committee

DEF
Professor Catedrático da Universidade de Aveiro (orientador)

GHI
Professor associado da Universidade J (co-orientador)

KLM
Professor Catedrático da Universidade N

agradecimentos / acknowledgements

Ágradecimento especial aos meus gatos...

Desejo também pedir desculpa a todos que tiveram de suportar o meu desinteresse pelas tarefas mundanas do dia-a-dia, ...

Abstract

An overlay network is a group of computational nodes that communicate with each other through a virtual or logic channel, built on top of another network. Although there are already numerous services and protocols implementing this mechanic, scalibility and administration agility are among the most desired characteristics of such a network topology. Hence, this document presents a centralized solution for the creation and control of secure overlay networks for multiple nodes - from client management to operation auditing. In the University of Aveiro, namely the autonomous robot ecosystem residing in the IRIS lab, supporting such a networking architecture would prove to be particular interesting, both for development and project organization. Therefore, this context is used as a validation environment. ...

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Network security has become a topic of evergrowing interest among any information system. Companies strive to ensure their communications follow principles of integrity and confidentially while minimizing attack vectors that could compromise services and data. With such goals in mind, network topologies are subjected to policies which apply rules and conditions to inbound and outbound traffic. One such mechanism is the use of vpn .

Traditional vpn services consist in the establishment of a secure, encrypted channel between a client and a network, through an insecure communication medium.

The ua's iris conducts research projects using autonomous mobile robots, which communicate through a Wi-Fi network. Currently, this network is confined to the premises of the iris, preventing the robots from operating in the remaining ua's buildings. Although the ua's Wi-Fi infrastructure covers most of its edifices, which can be used by the robots, due to security mechanisms, this network proves to be highly restraining, not allowing p2p communications through the ros - the operating system the robots run on - middleware without additional network equipments. Moreover, these constraints keep developers from being able to interact with the robots through their personal machines, which, if otherwise possible, would be of great interest.

1.2 Objectives

The main goal of this dissertation is to implement a private overlay network manager to be used exclusively by ua's clients. The concept of a manager entails both the definition of a network's client universe (which nodes should be allowed to connect to a certain network) and its respective identification and authentication mechanisms.

In the iris scenario, the management platform should provide operations to achieve communication between a team of robots, regardless of their physical location within the campus. Moreover, the authentication and connection to a desired overlay network by the robots must be a seemingless operation, requiring little to no manual configuration.

Finally, all traffic must be encrypted and properly authenticated, to ensure the privacy of the communication.

Chapter 2

State of the Art

This chapter covers the analysis and discussion not only of the motives and advantages behind the chosen tools and protocols to be used in this project but also but also of the common approaches and methodologies conducted in research in similar scenarios.

At its core, the system requires three main dimensions:

- A protocol for encrypted, reliable and efficient p2p communication
- A control platform for management of clients and authentication tokens
- A mechanism for scalibility, able to transform the many p2p channels into one mesh network

2.1 Encrypted Peer to Peer Communications / VPNs

2.1.1 Wireguard

[?] [?]

2.2 Control Platforms

2.2.1 Tailscale

2.2.2 Headscale

2.3 Mesh Networks

2.4 NAT Traversal

Bibliography

[1] Jason A. Donenfeld. WireGuard: Next Generation Kernel Network Tunnel.