Running HIP-VPLS in infrastructure mode

Dmitriy Kuptsov
2024

Table of contents

CHAPTER 1

Introduction

CHAPTER 2

Background

In this section we are going to describe some background material. We are going to start with the cryptographic primitives such as symmetric key encryption/decryption algorithms and then move on to the discussion of the Virtual Private LAN Services and what kind of problems they solve. We will then conclude the discussion in this chapter with the basic information on Host Identity Protocol as it is in the core of the solution which we are discussing in this document. To make the background material more or less complete we are going to touch alternative Transport Layer Security (we will here mention why this protocol is not used in the core of our architecture and is only used for the control-plane communications between the HIP-Switches and the HIP-controller). With these final words we are going to conclude current chapter of this work.

2.1 Cryptography

Cryptography forms the bases for secure telecommunications nowadays. SSL, TLS, SSH, Tacacs+, IPSec, DKIM, DNSSec are only few well-known telecommunication protocols that use cryptography to prevent such well-known attacks as eavesdropping, tampering, denial of message origin, etc. Modern cryptography is based on the hard-core mathematics and non-trivial algorithms (such as random number generation, discrete logarithm problem, rings, fields, Euclidean algorithm, factorization of big numbers, etc.)

2.1.1 Symmetric cryptography

Symmetric key cryptography is just perfect for the data-plane traffic as it offers high-processing times (when compare to asymmetric key cryptography). As the name implies, symmetric key cryptography uses the same secret key to encrypt and decrypt messages. On one hand it is the main reason why these algorithms are so fast. On the other hand, and this is the main limitation of the type of cryptography: symmetric keys are hard to distribute and revoke without using more sophisticated symmetric key schemes.

As of today several symmetric key cryptography algorithms, such as Advanced Encryption Standard (AES), Tripple DES (3DES), and Twofish offer advantageous processing speed and sufficient security levels. In our prototype implementation of HIP-VPLS we are using AES with 256 bits keys to perform encryption and decryption of data-plane traffic. Moreover, since NanoPI R2S - hardware that we employ to run our Software Defined Network (SDN) code - has support for on-chip instructions to boost the encryption and decryption of arbitrary long message blocks. In other words we do perform AES operations directly in the Central Processing Unit (CPU) of the tiny computer. We are going to devote a separate section on the implementation of the hardware accelerated AES encryption and decryption routines by the CPU.

2.1.2 Asymmetric cryptography

Asymmetric key cryptography as the name suggests uses two separate keys to encrypt and decrypt the messages. Since the encryption uses big number exponentiations (such as RSA) and multiplications (such as EDDSA), as well as modular arthihmetics, the performance of these types of algorithms is considerably worse when compared to symmetric cryptography algorithms.

However, since one is allowed to expose public part of the key to anyone, and since this key is only required to encrypt the message and only person who holds the private part of the key (secret part of the key) can decrypt the message, efficient key distribution and revocation can be organized, at the cost of extra CPU cycles. Moreover, by encrypting the message with the private key, and then making decryption plausible only with a public key (exposed to everyone), digital signature schemes can be implemented at no hassle.

2.1.3 Hash functions

2.1.4 Key exchange protocols

2.2 Virtual Private LAN Service

2.3 Host Identity Protocol

CHAPTER 3

Architecture

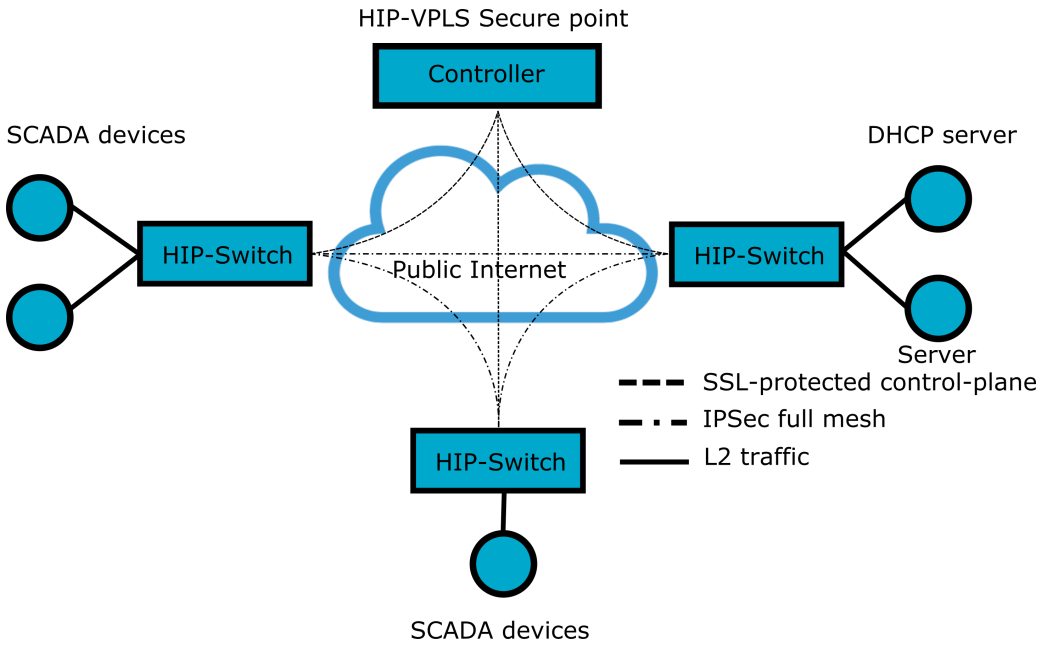

Figure 3.1: System architecture

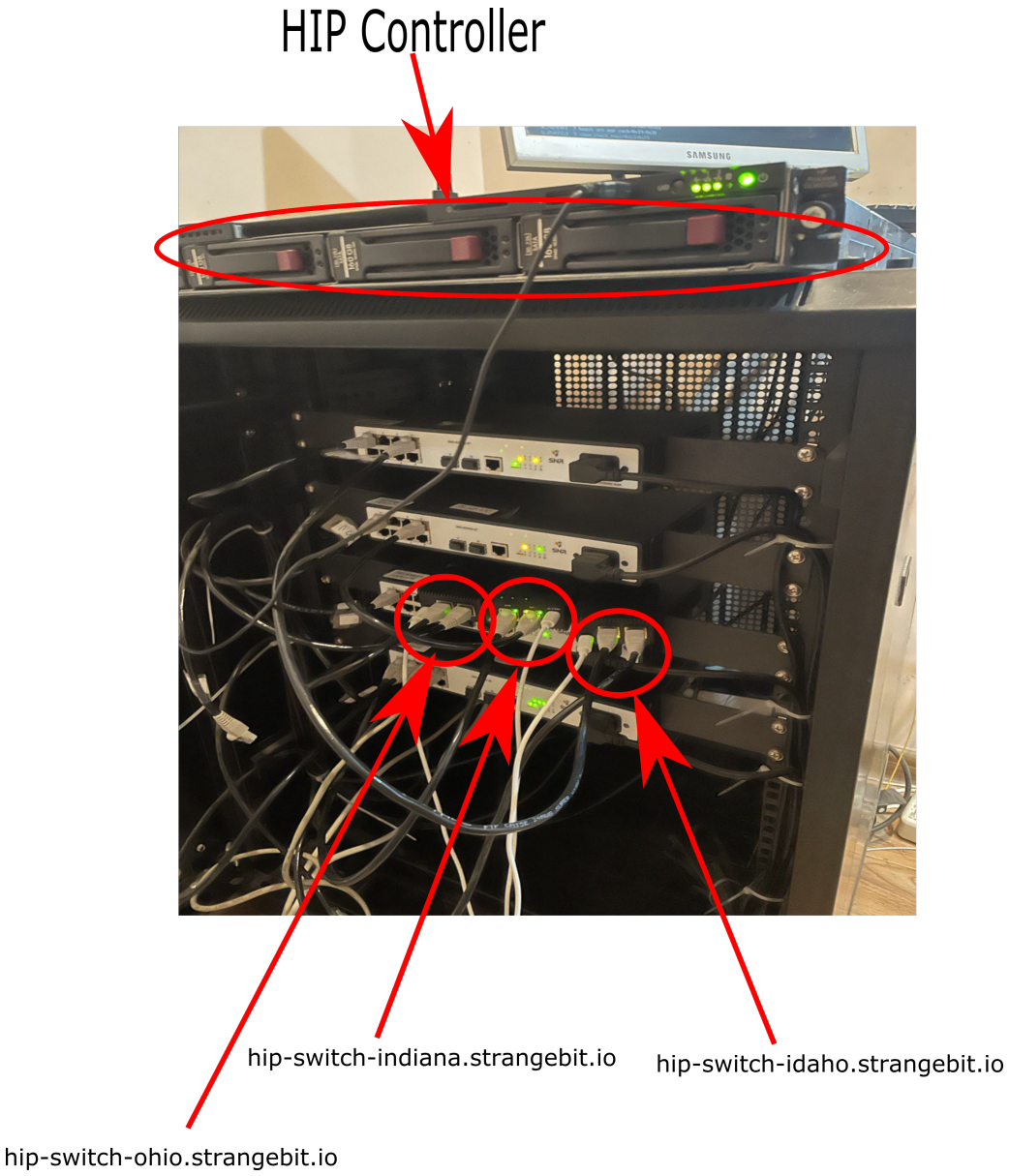

Figure 3.2: Testbed setup

Literature