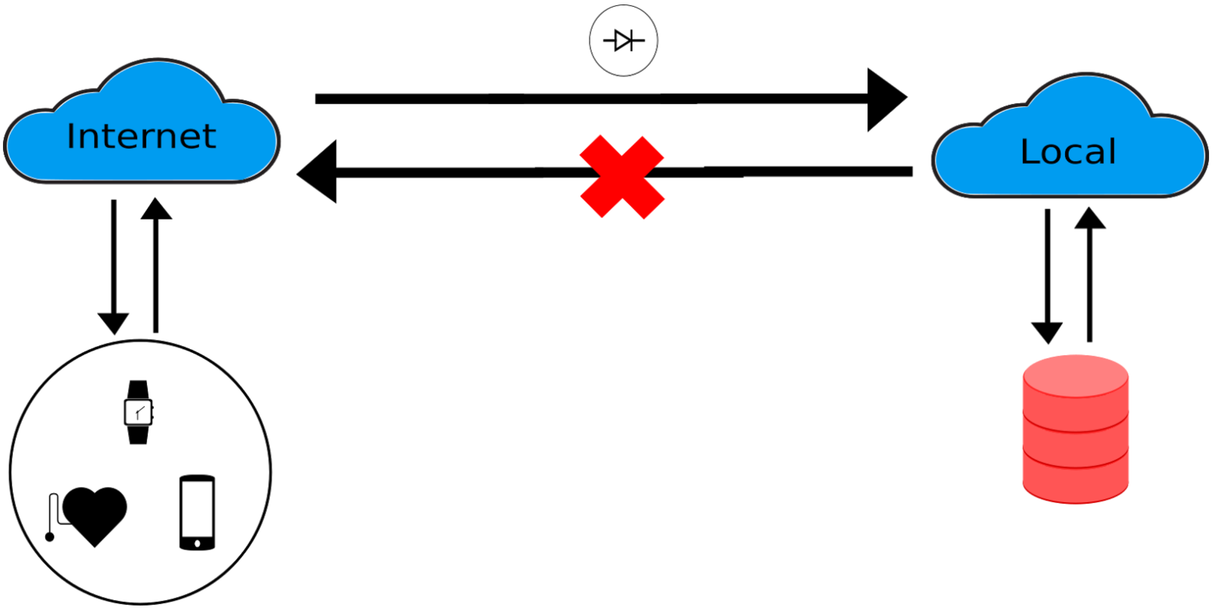
Management of security

Secure way to store sensitive data using data diode

CONOPS



Auteurs :
DANHIER Pierre
LECOCQ Alexis
NYAKI Loïc

Professeurs :
MEES Wim
DEBATTY Thibault

Introduction

When we need to protect sensitive data, the most common measure is to isolate our network from the internet. Acting this way ensure that the processed data are out of range from any outside opponent.

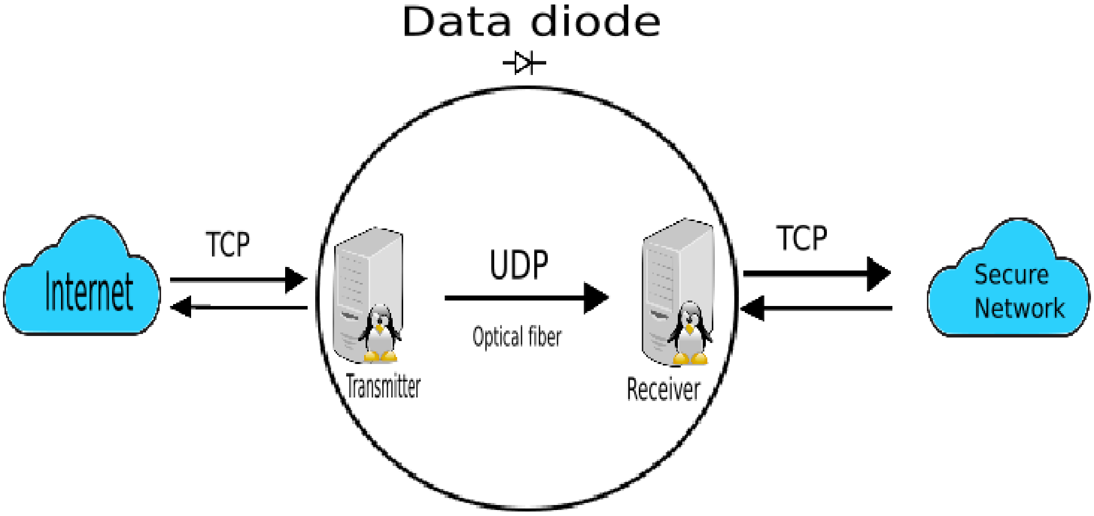
But when the process require some external informations, the manual import (via USB stick or other data transfer device) can compromise the security of the network. The device could contain malwares or sensitive data could be copied on it. Another drawback of the manual method is the human workload it requires. We then need a secure and automated data import system.

Context

In a more and more connected world, doctors want to get access to sensitive medical data generated by patient's devices. Those data could be heart frequency, sugar level within blood, body temperature or anything else (your imagination is the limit). Those data often come from connected devices worn by patients. We propose then to create a network where data can be received from but cannot be send to the internet. In other words we propose to install a data diode between the internet and our isolated network.

Data diode

A data diode is a secure one-way data transfer system. It guarantees the security by containing only one hardware one-way data transfer channel such as optical fiber. This system will then receive data from internet and send it to our secure network but will securely forbid data to leave our network for the internet.



Technical aspects

The data diode is composed of two servers linked by a one-way communication channel. The server A receives data from the internet with the TCP protocol . The integrity of the received data is then guaranteed. The server B uses TCP protocol to send data to the secure network too. The same conclusion can then be applied to those data.
The one-way communication channel forbids us to use the same protocol because TCP needs to send an acknowledgement of receipt to the sender. With a one-way communication channel, this is impossible. We will then use UDP for the communication between our two servers. The problem with UDP is that the sender cannot be sure that the receiver received the data or if the data is not corrupted. To mitigate this risk we chose to send three times the packets of data.

Installation

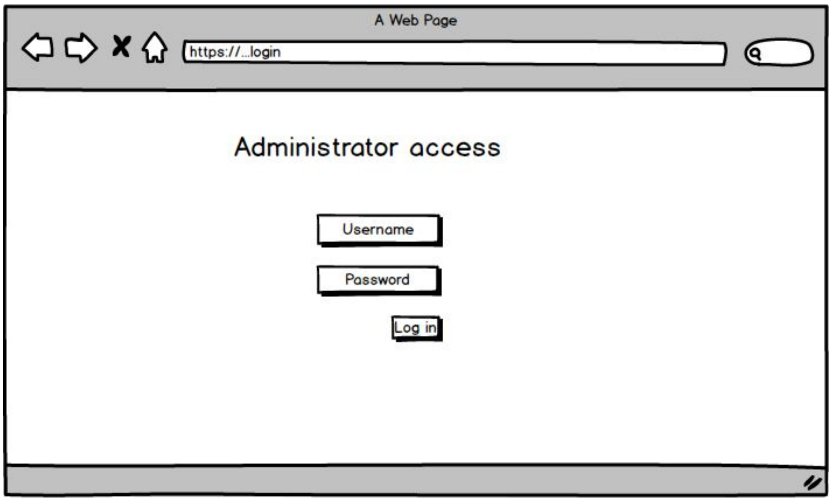
Plug the device's power cable to the AC then simply connect your internet router to the ethernet port A and your secure network router to the ethernet port B. The system settings are preconfigured.

Regular user

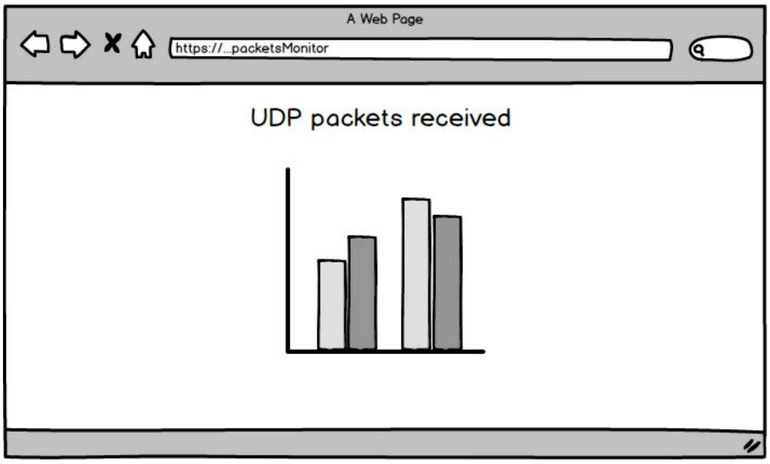
The only difference a regular user will see is that he will not be able to visit a external website anymore.

Administration

The system administration is done through a web interface only reachable from the secure network and with the correct login and password.



An administrator can monitor the rate of lost or corrupted packets between the two servers. A suddenly high rate can suggest a system malfunction. By default each packets is sent three times. For example, if the system only receives 2 times each packets, the link is certainly damaged .



He also can create or modify an administrator account. The informations for the first administrator account can be found in the box.