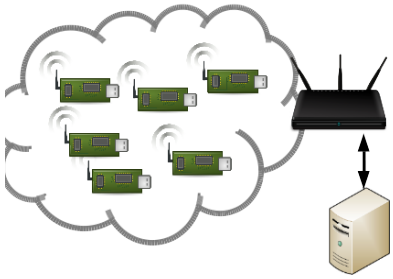
CS-E4300 Network Security, 2021-2022
Project 2
Teachers responsible for the project: Tuomas Aura, Aleksi Peltonen

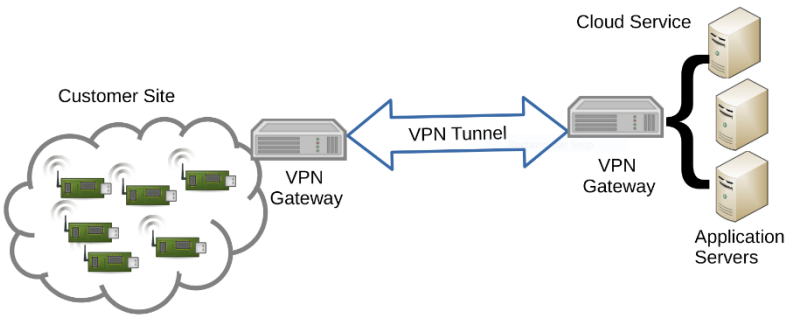
VPN from IoT devices to the cloud

In this exercise, you will act as a security and networking consultant and advice Acme Inc. on how to connect their sensor systems to the cloud.



Current setup of Acme's system is the following: At each customer site, IoT devices are connected to a local server through a wireless network (802.11 with WPA2 passphrase). The IoT devices report their status to the server periodically by connecting to TCP port 8080 on the server. The traffic volume is low, and delivery of the information is not time critical. The device-server connection is an insecure HTTP connection (REST API), and the devices do not support HTTPS. This is ok because both the devices and the server are in a local network that is isolated from the Internet by the wireless router's built-in NAT and firewall. A sketch of the current setup is here.

New plans: Acme has decided to migrate the servers from the customer sites to the cloud. This is expected to bring two advantages: (1) Easier remote administration of the server and no hardware maintenance. (2) The number of server instances can be reduced to one or a very small number. A very rough sketch of the expected configuration is shown here.



Acme wants your help to set up the IPsec VPN tunnels between the customer sites and the cloud service. On each customer site, a wireless AP will be connected to a VPN gateway, which is a Linux router. On the cloud side, the setup must work entirely on Linux virtual machines. The cloud-side setup should be scalable so that more server instances can be added in the future.

There are some constraints created by the fact that the different parts of the system come from different vendors: The IoT devices themselves cannot be modified, except by reconfiguring the IP address and port of the server, and it would be desirable to avoid even this manual configuration task. The modifications to the application server should also be kept to minimum because it is third-party software and customized versions can be expensive to maintain.

Your goal is to design and implement the IPsec-based VPN setup for this system.

You can do the prototyping in a virtual environment. Scripts and instructions for setting up a virtual network environment in **VirtualBox** and **Vagrant** are at https://github.com/tuomaura/cs-e4300_testbed. While these tools support Linux, Windows and MacOS, the setup may require some tuning for your own computer. You will have to choose and install the IPsec VPN software yourself (*strongSwan* is the common choice). For the project submission, please package your solution to small number of scripts, configuration files and instructions for deploying these on top of the above testbed.