VPN Tunneling

Arthur Carels, Oksana Baranova

January 11, 2021

1 Understanding the problem

IoT devices on the client side periodically connect to their local server via TCP port 8080. The used connection is not secure enough due to the use of the HTTP protocol, which has security flaws in comparison to HTTPs. While the clients are in the local (safe) network, the additional security is not required. However, because of the need for migration of the servers from (local) customer sites to the cloud, the presence of a secure communication channel is needed.

2 Solution

To ensure secure communication, a VPN tunnel between the clients (i.e. sensors) and cloud is used. The VPN-tunnel has been configured with password authentication using the StrongSwan tool, which is most popular for Linux OS.

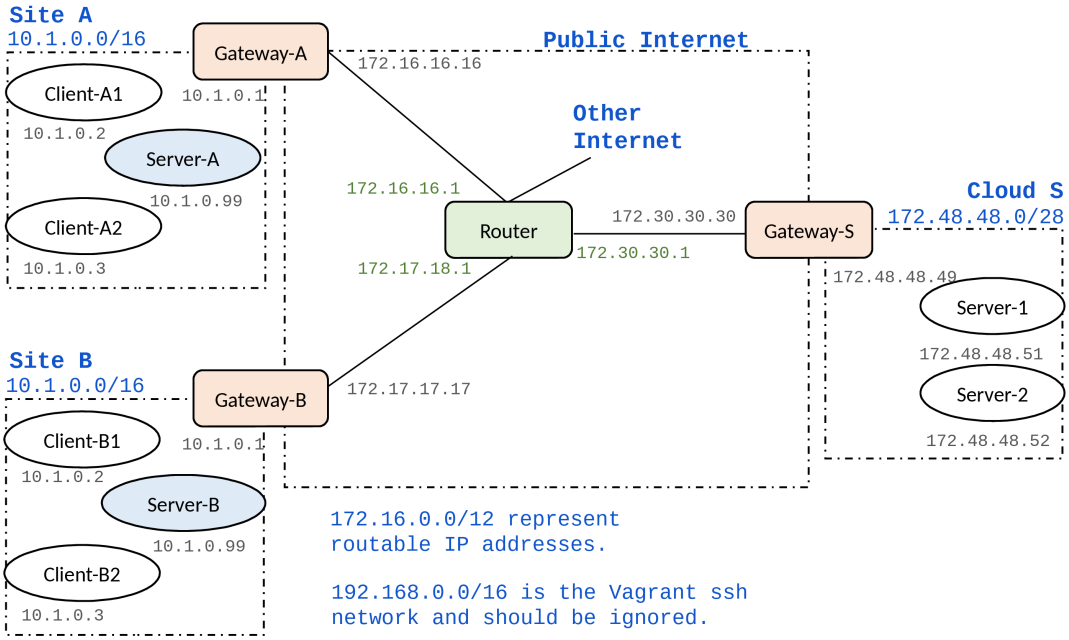

Figure 1: Original network overview

2.1 Goals

The main goal is to relocate the server functionality from the client's (local) network to a cloud platform and ensure the proper level of security of the traffic going over the network. The network connectivity has

2.2 Implementation

The IPSec (Internet Protocol Security) Protocol Suite is a set of network security protocols to ensure the security of data traffic over TCP/IP network. In this assignment, a demonstration of how to setup and configure the IPSec-based VPN-tunnel was made. IPsec includes the *Authentication Header* (AH) protocol to carry out authentication and integrity, the *Encapsulation Security Payload* (ESP) protocol to ensure encryption of IP packets and the *Internet Security Association and Key Management Protocol* (ISAKMP) for secure key exchange over the Internet.

Parameters	**Client A**	**Client B**
key distribution method	ISAKMP	ISAKMP
encryption algorithm	AES-256	AES-256
hash algorithm	SHA2-256	SHA2-256
authentication method	password	password
key exchange	DH	DH
IKE SA lifetime	1h	1h
ESP transform encryption	esp-aes	esp-aes
ESP transform authentication	esp-sha2	esp-sha2
Traffic to be encrypted	172.16.16.16-172.30.30.30	172.17.17.17-172.30.30.30
SA Establishment	ipsec-isakmp	ipsec-isakmp

Table 1: IpSec Policy Parameters

For better security and saving on IPv4 addresses, a private network was created on the cloud side with the 10.2.0.0/16 address space. When configuring the tunnel, the password authentication method was selected. Configuration settings were created on gateways A, B and S via `sudo nano /etc/ipsec.conf` (see Table 1) and `sudo nano /etc/ipsec.secrets` commands. Secrets were created via command: `head -c 24/dev/urandom | base64`.

Iptables is a command line utility for managing the IP packet routing rules for the Linux kernel firewall, which is used to set up the traffic flow procedure. *Network Address Translation* (NAT) provides the ability for packets to transfer from the internal (private) network through the gateway to the Internet (translation of network addresses of transit packets). In order to access the Internet, clients communicate with servers via their (default) gateways A and B. The gateway listens for packets coming from the Internet on a specific interface enp0s8 and redirects them to the correct machines on the local network.

To check the traffic encryption the command `sudo tcpdump -i <interface>}` was used. The result has shown that ESP guarantees the encryption of the traffic and the tunnel was constructed correctly.

3 Conclusion

VPN tunnels are used for secure transmission of data over the Internet public network. To avoid potential security threats, the VPN tunnel has been constructed with a number of advanced encryption algorithms to provide confidentiality of the data transmitted between sides. Thus, the initial problem of secure transferring services to the cloud has been solved.