

Case study:

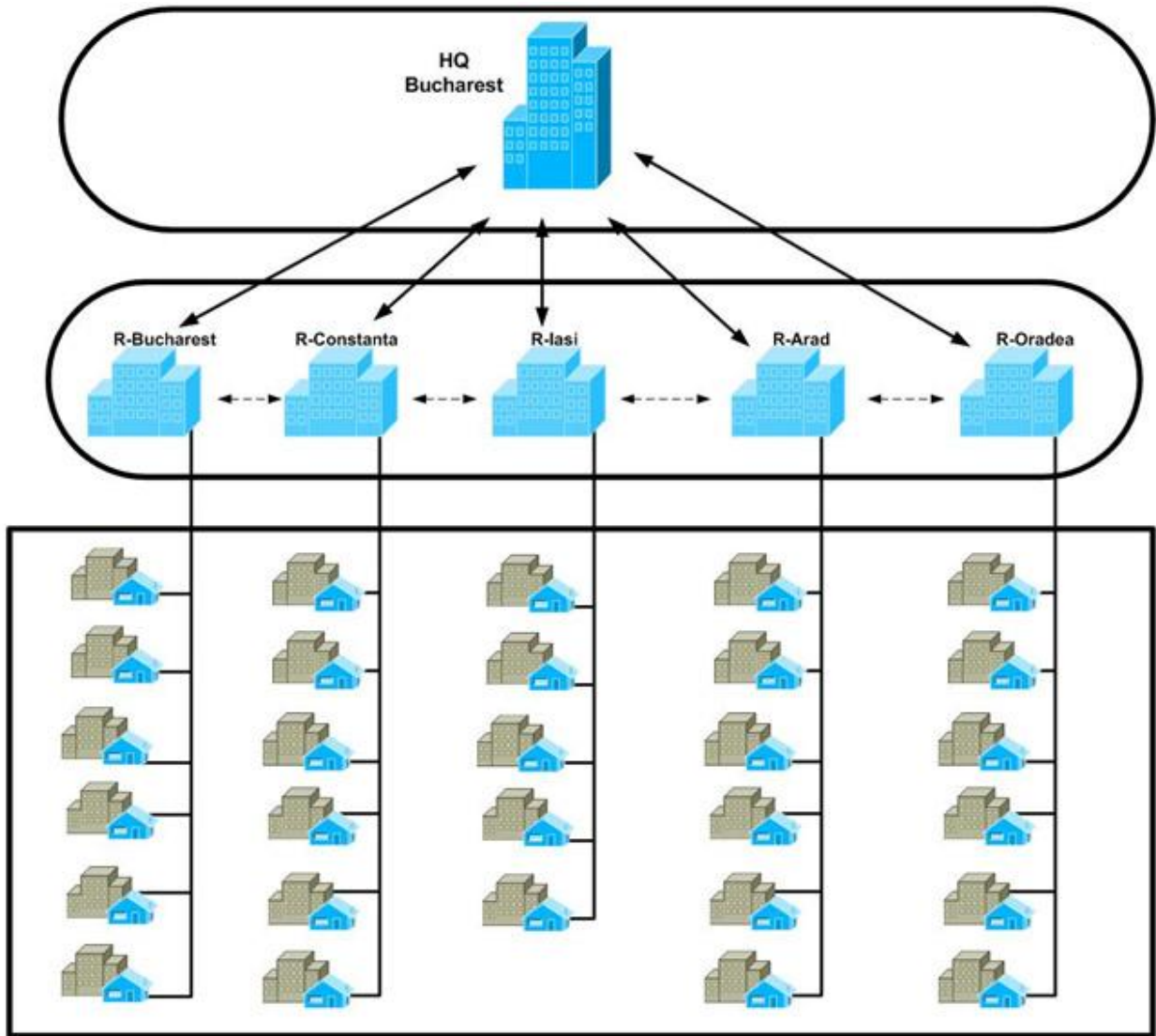
One of our currently supported customers, where we have projected, implemented and configured the network is a major Romanian public company which has a nation wide network, with about 20 regional offices, which gather the traffic from about 100 local offices. All the data is concentrated to Head Quarter location, where the main servers are and the internet access is located.

All of the locations are secured by a firewall solution which protects internal servers and internal users by the potentially intruders and also realizes a parallelization of traffic (traffic is filtered and quality of services is applied to it).

Special VPN equipments encrypt the links between all locations, by creating encrypted tunnels concentrated in a VPN Gateway located in the HQ location. This way all communication is protected by all possible intruders or by man-in-the middle attacks, meaning nobody can intercept the traffic or if he does, it would take years to decrypt it. This way, the users from the customs and regional offices can connect to servers located into the HQ network as if they would be locally, without being worried about security of data or about the fact that somebody might attack them.

The HQ contains a VPN gateway and a firewall solution, which contains more level of security, each of them protecting a different part of the HQ's network, one with servers, one with internal users, and many other networks with Customs specific needs. Also at the HQ is implemented a VPN solution based on remote users connections, meaning the users can connect from all over the internet based on digital certificates and gaining access to servers located inside the Customs network. They will establish an encrypted tunnel with the VPN gateway, receiving an IP address they will use to connect to the inside servers they need.

The architecture of the whole network looks like the one below:



LEGEND

