VoIPBullGuard
Présentation

What is the purpose of VoIPBullGuard ?

Each time a VoIP server enter in production, VoIP hackers began to try attacks in order to enter inside it, using automatic softwares wich proceed in several steps.

VoIPBullGuard mission is to protect VoIP servers against attacks on **ssh port**, **l5060 port** (VoIP) and **80 port** (Apache server)

VoIPBullGuard uses **fail2ban** et **iptables**, two software of **Linux CentOS**.

VoIPBullGuard permit to defend automatically your server, sometimes before a try of an hacker, because all the servers of our customers centralise attacks in our main server.

Remark : Hackers attacks on 80 port intend to enter inside your billing system or the phpmyadmin interface in order to steal VoIP account. Those numerous hackers tries exhausts the processor of your server, and full the logfile of:

- your billing system
- the Apache server
- your linux secure, messages and fail2ban logfiles

What can NOT do VoIPBullGuard ?

VoIPBulGuard can not protect you against the stealing of:

- your billing login & password
- your ssh login & password
- your phpmyadmin login & password

if you have a trojan horse inside your windows personal computer, or if you work in a cybercafe, if you use a wifi-connection without a strong security at home, of if you use a wifi-connection in a public area or in a hotel while travelling.

We advise to have on your personal computer a good antivirus with regular update, and a software provided by **Emsisoft**. (very useful against trojan horses)

Please be very careful when you download free softwares, wich contains sometimes trojanhorses and unwanted adverstising systems.

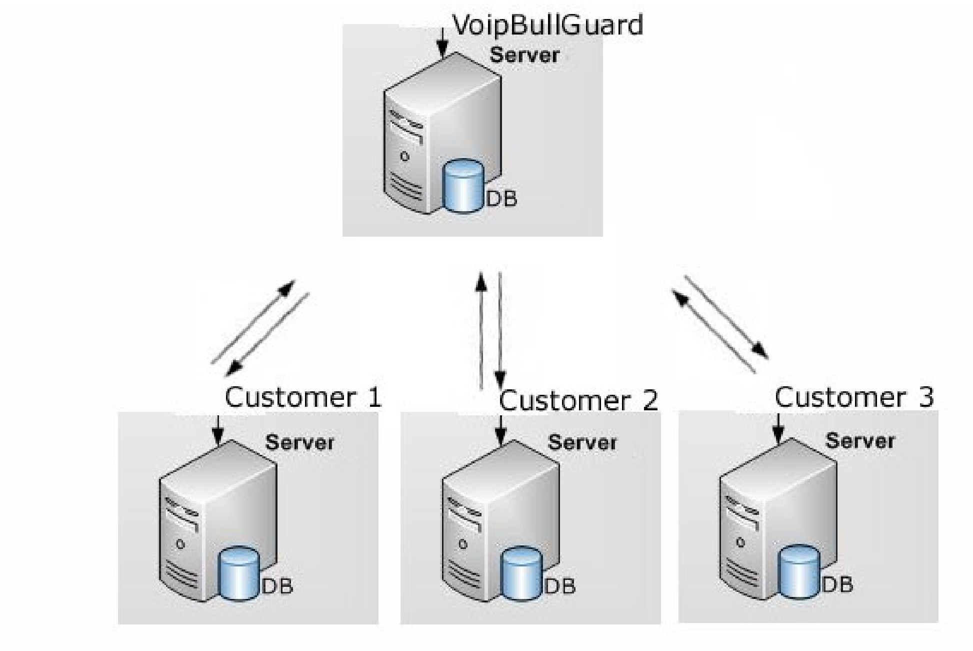
How works VoIPBullGuard ?

The fail2ban softwares of our customers send by email all suspects hackers ip to our Main Server.

Our Main Server maintain a database of VoIP hackers, updated each day.

Our webmaster check all suspect ip, and decides if they have to be blocked by the servers of our customers.

Then our Main Server send requests to the servers of our customers (maximum 5 ip each day is enough), and the servers of our customers add those hackers ip to the iptables file, in order to stop those ip.



How to activate this service ?

→ Or you provide us SSH access to your server, and we install the required system. After that, you can change your SSH password.

→ Or we send us a detailed procedure to activate our system yourselve. In this case, we do not need a SSH access. By evidence, you must have a minimum experience of linux Operating systems and required linux command to achieve this operation.

Advantages of our system:

→ We are advised of hackers VoIP attacks by more than 60 VoIP servers

→ Your informaticians staff does'nt have to loose times to modify the iptables configuration regularly, wich is costly.

Tarification

- 60,00 euros per month TTC,

- 180,00 euros TTC at our first technical intervention, if we have to securize ourselves your server (add a secondary ssh account, desactivating of a direct SSH root access, configuration of fail2ban to send email to our Main Server, configuration of our system inside your server)