

LINUX - Life in the console IS!!! Configuring iptables firewall on the server acting as the Internet gateway

Login Password Remember me It's not quite finalized article configuration in the testing process So at one point there was a need to set the firewall on the server under Linux which will be the Internet gateway and beyond. Main tasks - close the access of employees to certain sites - SOC. network and other not closing them for the bosses. - close the ICQ is a chat for employees also leaving access to her superiors. - prohibit access to the network of other potentially unwanted applications. - make a port forwarding for the ability of it Department to connect to their work computer from external network. - to access from outside to the server for administration using ssh. - to open from outside 80ый port for access to future website. - to open from outside ports 25 and 110 to your mail server. - For IT departments to separately open all that you will need In the end, employees in external network open only ports 80 http, 443 https, 53 dns and closed vkontaktiki etc.. ICQ will not work as they use ports. primary 5190. To implement these tasks will be using the iptables command-line utility is a standard interface for managing firewalls firewall netfilter for Linux kernel versions 2.4 and 2.6. After a day exploring was created a fairly simple setup script, probably not without drawbacks but it is working. The theory of copy-paste will not online in its sea and from the comments below, much appreciated. Let's get started. If iptables is not installed - put `sudo su apt-get install iptables` Create setup script and give the rights to execute it `touch fw.sh chmod +x fw.sh` Create two text files. one will be kept a vip list of ip addresses which will be available to all sites in the second list of banned sites `touch sbd.txt touch ipbd.txt` and fill them `nano sbd.txt vkontakte.ru durov.ru vk.com odnoklassniki.ru and other.... nano ipbd.txt 10.10.10.10 10.10.10.11 etc.` Next, go to the script settings. We have the following local network 10.10.10.0/24 on the network adapter eth1 is external network adapter, eth0 c ip for example 88.45.65.2. `nano fw.sh` binbash Variables specify the external ip of the server and externally. `network interface INETIP1=88.45.65.2 INETIFACE1=eth0` specify the internal ip of the server and EXT. `network interface LANIP=10.10.10.4 LANIFACE=eth1` internal network `LANRANGE=10.10.10.0/24 network interface loop and ip LOIFACE=lo LOIP=127.0.0.1` IP address in LAN which is doing the forwarding `IPFORW1=10.10.10.57 external port PORTV1=3389 internal port PORTI1=3389 PRTCL1=tcp IPFORW2=10.10.10.50 external port PORTV1=3489 internal port PORTI1=3389 PRTCL2=tcp ip=iptables` specify the path to the text file containing the list of banned sites `badsite= $cat homevirtdiversbd.txt` specify the path to the text file containing the list of ip for which all sites are open `goodip= $cat homevirtdiveripbd.txt`

Link to article:: [LINUX - Life in the console IS!!! Configuring iptables firewall on the server acting as the Internet gateway](#)