برای پیکر بندی فایروال لینوکس CentOS جهت نرم افزار IBSng کارهای زیر را انجام دهید.

این کار را با دستورات iptables انجام می دهم. برای کانفیگ فایروال لینوکس جهت نرم افزار IBSng دو راه وجود دارد.

۱. غیر فعال کردن فایروال لینوکس .CentOS با اینکار سطح امنیتی لینوکس پایین می آید. در آموزش های زیادی که دیدم فایروال رو غیرفعال می کردند .
۲. باز کردن پورت های مربوط به IBSng که این کار توصیه می شود .

👍غیر فعال کردن فایروال

برای این کار دستور زیر را وارد کنید.

```
1                    ***
2 service iptables stop
3 ***
```

با غیر فعال کردن Firewall سطح امنیتی لینوکس پایین می آید.

👍پیکربندی فایروال لینوکس با باز کردن پورت IBSng روی لینوکس

.1مرحله اول از پیکربندی فایروال را با کد های زیر آغاز می کنم.

```
1       ***
2 sysctl -p
3 echo 1 /proc/sys/net/ipv4/ip_forward
4                                  ***
```

- در خط اول با دستور sysctl –p یک سری از پارامتر های هسته کرنل لینوکس را می بینیم .

```
[root@l0ve ~]# sysctl -p
net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
error: "net.bridge.bridge-nf-call-ip6tables" is an unknown key
error: "net.bridge.bridge-nf-call-iptables" is an unknown key
error: "net.bridge.bridge-nf-call-arptables" is an unknown key
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 4294967295
kernel.shmall = 268435456
[root@l0ve ~]# _
```

در اینجا مقدار پارامتر net.ipv4.ip_forward = 0 است. ۰ شدن آن یعنی اینکه بسته هایی که به کارت شبکه ارسال می شوند، از بین رفته و به مقصد Forwardنمی شوند. پس باید مقدار آن به ۱ تغییر کند. برای این کار از دستور خط دوم استفاده کنید.

- در خط دوم مقدار پارامتر ip_forward به ۱ تغییر می کند. برای Forward کردن بسته های ارسال شده به کارت های شبکه دیگر در لینوکس باید مقدار این پارامتر برابر ۱ شود. یک مشکل وجود دارد این است که این تنظیم موقتی خواهد بود. با ریستارت شدن لینوکس از بین می رود .

برای رفع این مشکل کد زیر را وارد کنید.

```
1                    ***
2 nano /etc/sysctl.conf
3 ***
```

با دستور بالا فایل sysctl.conf در ویرایشگر nano باز می شود. پارامتر ip_forwardرا پیدا کنید و مقدار ۰ را به ۱ تغییر می دهید. سپس Ctrl+X را بگیرید y .را تایپ کنید Enter .را فشار دهید.

```
  GNU nano 2.0.9            File: /etc/sysctl.conf

# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8)
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the ker
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core fi
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ? _
 Y Yes
 N No            ^C Cancel
```

برای مشاهده تغییرات کد های زیر را وارد کنید.

```
1    ***
2 reboot
3 sysctl net/ipv4/ip_forward
4                        ***
```

با کد reboot لینوکس ریستارت می شود. بعد از اینکه لینوکس بوت شد و بالا آمد برای مشاهده تغییرات با استفاده از کد خط دوم می بینید که مقدار پارانتر ip_forward به ۱ تغییر پیدا کرده است.

```
[root@l0ve ~]# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
[root@l0ve ~]# _
```

.2مرحله دوم از کانفیگ فایروال لینوکس را با کد های زیر ادامه می دهم.

یادآوری

پورت های IBSng ، پورت ۱۸۱۲ و ۱۸۱۳ می باشند. لازم است بدانید در حالت معمول نیازی به تغییری در فایروال نداریم. اما اگر در مواقعی نیاز شد که دو پورت IBSng باز شوند کد های زیر را وارد کنید.

```
1                                                                    ***
2 iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 1812 -j ACCEPT
3 iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 1813 -j ACCEPT
4                                                  service iptables save
5 ***
```

یادآوری

اگر شما از سرور PPTP برای اتصال به IBSng استفاده می کنید باز کردن پورت ۱۷۲۳ و نوشتن Rule های زیر الزامی است ولی در حالت معمول نصب IBSng به این کدها نیازی نیست.

```
1                                                  ***
2 iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
3 iptables -A INPUT -i eth0 -p tcp -dport 1723 -j ACCEPT
4             iptables -A INPUT -i eth0 -p gre -j ACCEPT
5 iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
6 iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT
7 iptables -t filter -I FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN
8                  -m tcpmss --mss 1300:8000 -j TCPMSS --set-mss 1300
 9 service iptables save
10                  ***
```

- در خط اول دستور iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE را وارد کنید .

-t nat برای ترجمه آدرس استفاده می شود -t .مخفف —table است -A .مخفف appendیا add است .
POSTROUTINGبرای تغییر آدرس مبدا به کار می رود -o .مخفف —out –interface است eth0 .هم خود اینترفیس خروجی لینوکس است -j MASQUERADE .یک rule یا قانون برای chain یا زنجیر POSTROUTING است.

با این دستور تمامی بسته های فرستاده شده از سرویس های داخل لینوکس به اینترفیسeth0 ، به آیپی ۱۹۲.۱۶۸.۱.۱۹ تغییر آیپی می دهند. یعنی آیپی سرویس های مبدا به این آیپی ترجمه می شوند.

- در خط دوم دستور iptables -A INPUT -i eth0 -p tcp –dport 1723 -j ACCEPT را وارد کنید .

از زنجیر INPUT برای فیلترینگ بسته هایی که داخل لینوکس می شوند استفاده می شود -i eth0 .مخفف– in —interfaceاست eth0 .هم که اینترفیس خروجی است -p tcp .هم مخفف پروتکل tcp است -dport .هم پورت مقصد را مشخص می کند -j ACCEPT .هم یک rul یا قانون است.

پورت ۱۷۲۳ متعلق به نرم افزار IBSng نصب شده روی لینوکس است. با استفاده از کد بالا، بسته هایی که از خارج وارد لینوکس می شوند و از پروتکل tcp تبعیت می کنند با استفاده از این پورت به سمت IBSng هدایت می شوند

- در خط سوم دستور iptables -A INPUT -i eth0 -p gre -j ACCEPT را وارد کنید .

در این دستور اگر بسته ای از خارج به سمت اینترفیس eth0 لینوکس برود و از پروتکل gre که یک پروتکل امنیتی ppp است، تبعیت کند، با rule یا قانون ACCEPTاجازه ورود پیدا می کند.

- در خط چهارم دستور iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT را وارد کنید .
- در خط پنجم دستور iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT را وارد کنید .

از این دو دستور برای Forward بسته های ppp استفاده می شود. آدرس های مبدا و مقصد eth0 و سرویس ppp است. از FORWARDبرای ارسال بسته ها بین کارت های شبکه استفاده می شود.

- در خط ششم در جدول filter تنظیماتی برای Forward شدن بسته ها اعمال می شود. به علت طولانی بودن این کد آن را در دو خط نوشتم .
- در خط آخر دستور service iptables save را برای ذخیره کردن دستور های بالا وارد کنید .

در شکل زیر روش وارد کردن کد ها را می بینید.

```
[root@vpn ~]# iptables -A INPUT -i eth0 -p tcp --dport 1723 -j ACCEPT
[root@vpn ~]# iptables -A INPUT -i eth0 -p gre -j ACCEPT
[root@vpn ~]# iptables -t filter -I FORWARD -p tcp -m tcp --tcp-flags
SYN,RST SYN -m tcpmss --mss 1300:8000 -j TCPMSS --set-mss
[root@vpn ~]# iptables -A FORWARD -i eth0 -o ppp+ -j ACCEPT
[root@vpn ~]# iptables -A FORWARD -i ppp+ -o eth0 -j ACCEPT
[root@vpn ~]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@vpn ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

نکته

اگر دستور خط ششم را بدرستی وارد نکنید، یوزر هایی که به سرور وصل می شوند، می توانند به سرور وبسایت پینگ داشته باشند ولی نمی توانند آن وبسایت را باز کنند.

نکته

اگر در فایل iptables کدهایی بودند که packet ها رو reject می کنند اون ها رو پاک کنید. مثلا در شکل زیر کدی هست که packetها رو reject می کند .این هایی که به Reject ختم می شوند رو پاک کنید.

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [8:896]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 1723 -j ACCEPT
-A INPUT -i eth0 -p gre -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -i eth0 -o ppp+ -j ACCEPT
-A FORWARD -i ppp+ -o eth0 -j ACCEPT
COMMIT
# Completed on Sat May  5 05:38:14 2012
```

نکته

اگر می خواهید تنظیمات انجام شده را ببینید و از صحت کار خود مطمئن شوید از کد زیر استفاده کنید.

```
1                                ***
2 nano /etc/sysconfig/iptables
3 ***
```

در شکل زیر می توانید این تنظیمات را ببینید.

```
  GNU nano 2.0.9                                    File: /etc/sysconfig/iptables

# Generated by iptables-save v1.4.7 on Sun May  6 17:39:14 2012
*filter
:INPUT ACCEPT [34:2488]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [24:2288]
-A INPUT -p icmp -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 1723 -j ACCEPT
-A INPUT -i eth0 -p gre -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1300:8000 -j TCPMSS --set-mss 1300
-A FORWARD -i eth0 -o ppp+ -j ACCEPT
-A FORWARD -i ppp+ -o eth0 -j ACCEPT
COMMIT
# Completed on Sun May  6 17:39:14 2012
# Generated by iptables-save v1.4.7 on Sun May  6 17:39:14 2012
*nat
:PREROUTING ACCEPT [201:13814]
:POSTROUTING ACCEPT [80:5091]
:OUTPUT ACCEPT [83:5330]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Sun May  6 17:39:14 2012
```