? iptables ????????? FreePBX ?? fail2ban ?????????????????

??? iptables ??
???? IP??????

iptables -A INPUT -i eth0 -s 111.222.333.444 -d 192.168.1.100 -j DROP

iptables -A INPUT -i eth0 -s 111.222.333.0/24 -d 192.168.1.100 -j DROP

TIPs:

- 192.168.1.100 ? Asterisk ? ?? IP
- ?????:
  111.222.333.0/24
  111.222.0.0/16
  111.0.0.0/8

???????

iptables -D INPUT -i eth0 -s 111.222.333.444 -d 192.168.1.100 -j DROP

TIPs:

- ?????????????

for CentOS
(http://sysadminman.net/blog/2009/ipt...nd-freepbx-772)
?? /etc/sysconfig/iptables

iptables:

```
*filter
:INPUT DROP [636:118995]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [45625:6667023]
:fail2ban-APACHE - [0:0]
:fail2ban-ASTERISK - [0:0]
:fail2ban-BadBots - [0:0]
:fail2ban-SSH - [0:0]
:fail2ban-VSFTPD - [0:0]
-A INPUT -p tcp -m multiport --dports 80,443 -j fail2ban-BadBots
-A INPUT -p tcp -m tcp --dport 21 -j fail2ban-VSFTPD
-A INPUT -p tcp -j fail2ban-APACHE
-A INPUT -j fail2ban-ASTERISK
```

```
-A INPUT -p tcp -m tcp --dport 22 -j fail2ban-SSH
-A INPUT -i ! eth0 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT
-A INPUT -m state --state ESTABLISHED -j ACCEPT
-A INPUT -m state --state RELATED -j ACCEPT
-A INPUT -p udp -m udp --sport 53 --dport 1024:65535 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 113 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 9001 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 9080 -j ACCEPT
-A INPUT -p udp -m udp --dport 4569 -j ACCEPT
-A INPUT -p udp -m udp --dport 5000:5082 -j ACCEPT
-A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 4445 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 5038 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -p udp -m udp --dport 69 -j ACCEPT
-A fail2ban-APACHE -j RETURN
-A fail2ban-ASTERISK -j RETURN
-A fail2ban-BadBots -j RETURN
-A fail2ban-SSH -j RETURN
-A fail2ban-VSFTPD -j RETURN
COMMIT
# Completed on Tue Feb  8 11:35:49 2011
# Generated by iptables-save v1.3.5 on Tue Feb  8 11:35:49 2011
*mangle
:PREROUTING ACCEPT [59114:43092827]
:INPUT ACCEPT [58517:43020696]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [45625:6667023]
:POSTROUTING ACCEPT [45627:6667307]
COMMIT
# Completed on Tue Feb  8 11:35:49 2011
# Generated by iptables-save v1.3.5 on Tue Feb  8 11:35:49 2011
*nat
:PREROUTING ACCEPT [1620:224741]
:POSTROUTING ACCEPT [3827:274034]
:OUTPUT ACCEPT [3827:274034]
COMMIT
# Completed on Tue Feb  8 11:35:49 2011
```

?? iptables

service iptables stop
service iptables start

TIPs:

port 113 ?????????

port 4445 Flash Operator Panel

port 9001 webmin

port 9080 2nd Web port

port 4569 IAX2

port 5038 Asterisk Manager Interface

port 123 NTP

port 69 TFTP

????

- Arno's IPTABLES FIREWALL