



?? 11, 2009 ??? sunchiahome

? ? samba Server ?????24?????,????????????????????,????????,????? port ??,??????????  
 iptables(firewall) ? SELinux ????? Samba ??????.???????????????? iptables(firewall) ? SELinux.?Linux?????  
 iptables.?? RHEL5 ?? iptables ?????.????:

```
[root@benjr ~]#system-config-securitylevel
```

????: ??????????????(iptables)?????????  
 ?????????? port ??,????? port ??? SMB /NMB ??????????????.???NetBIOS  
**(UDP ports 137 and 138, TCP ports 139) ? TCP port 445 for SMB file sharing without NetBIOS.**

????????? SSH ?????????? Text mode ????

```
[root@benjr ~]#system-config-securitylevel-tui
```

????????,???????????????????? /etc/sysconfig/iptables

```
[root@benjr ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i ppp0 -j ACCEPT
-A RH-Firewall-1-INPUT -i eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

??:

?????? samba ?????? port.

```
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
????????? iptables ,?????????,????????????? iptables .
```

```
[root@benjr ~]#chkconfig iptables on
```

????????????????????????????????????? iptables ??.

```
[root@benjr ~]#service iptables start
Starting httpd [OK]
```

???? iptables ??????

```
[root@benjr ~]#/sbin/service iptables save
#????????? /etc/sysconfig/iptables
```

????????? : <http://benjr.tw/?q=node/444>