

---

Subject: \*SOLVED\* Firewall rule don't allow ftp while port 21 is open

Posted by [whatever](#) on Thu, 05 Oct 2006 10:03:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hello,

Below is the firewall script but it doesn't allow the ftp.

```
#!/bin/bash
```

```
IPTABLES="/sbin/iptables"
```

```
SERVER_IPS=`/sbin/ifconfig | grep inet | cut -d : -f 2 | cut -d \ -f 1 | grep -v 127.0.0.1`
```

```
FWIN="${IPTABLES} -A INPUT"
```

```
FWOUT="${IPTABLES} -A OUTPUT"
```

```
OK="-j ACCEPT"
```

```
NO="-j DROP"
```

```
# Flush tables and change default policy to DROP
```

```
function initialize() {  
    local TABLE="${1}"  
    ${IPTABLES} -F ${TABLE}  
    ${IPTABLES} -P ${TABLE} DROP  
}
```

```
# Flush tables and change default policy to ACCEPT
```

```
function stop() {  
    local TABLE="${1}"  
    ${IPTABLES} -F ${TABLE}  
    ${IPTABLES} -P ${TABLE} ACCEPT  
}
```

```
# Verify call switch
```

```
case "$1" in  
start|restart)
```

```
    initialize INPUT  
    initialize OUTPUT  
    initialize FORWARD
```

```
    # INPUT  
    # 1) loopback  
    ${FWIN} -i lo ${OK}  
    ${FWIN} -d 127.0.0.0/8 ${NO}
```

```
    # 2) We allow incoming SSH connections and answers to  
    # our own SSH connections:
```

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp -d ${OURIP} --dport 22 ${OK}
    ${FWIN} -p tcp --sport 22 -d ${OURIP} --dport 1024: "!" --syn ${OK}
done
```

# 3) We allow incoming DNS queries as well as answers to our  
# DNS queries.

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp -d ${OURIP} --dport 53 ${OK}
    ${FWIN} -p udp -d ${OURIP} --dport 53 ${OK}
    ${FWIN} -p tcp --sport 53 -d ${OURIP} --dport 1024: "!" --syn ${OK}
    ${FWIN} -p udp --sport 53 -d ${OURIP} --dport 1024: ${OK}
done
```

# 4) We allow access to our SMTP server, as well as answers  
# to our SMTP connections and, temporarily, identd stuff:

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp -d ${OURIP} --dport 25 ${OK}
    ${FWIN} -p tcp --sport 25 -d ${OURIP} --dport 1024: "!" --syn ${OK}
    ${FWIN} -p tcp --sport 1024: -d ${OURIP} --dport 113 ${OK}
    #${FWIN} -p udp --sport 1024: -d ${OURIP} --dport 113 ${OK}
    ${FWIN} -p tcp --sport 113 -d ${OURIP} --dport 1024: "!" --syn ${OK}
    #${FWIN} -p udp --sport 113 -d ${OURIP} --dport 1024: ${OK}
done
```

# 5) We also allow access to our POP/sPOP server.

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp -d ${OURIP} --dport 110 ${OK}
    ${FWIN} -p tcp -d ${OURIP} --dport 995 ${OK}
done
```

# 6) and to IMAP/IMAPs

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp -d ${OURIP} --dport 143 ${OK}
    ${FWIN} -p tcp -d ${OURIP} --dport 993 ${OK}
done
```

# 7) we would like to be able to use lynx ;)

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p tcp --sport 80 -d ${OURIP} --dport 1024: "!" --syn ${OK}
done
```

# 8) We allow incoming echo replies/requests from everywhere:

```
for OURIP in ${SERVER_IPS}; do
    ${FWIN} -p icmp -d ${OURIP} --icmp-type 0 ${OK}
    ${FWIN} -p icmp -d ${OURIP} --icmp-type 3 ${OK}
    ${FWIN} -p icmp -d ${OURIP} --icmp-type 8 ${OK}
    ${FWIN} -p icmp -d ${OURIP} --icmp-type 11 ${OK}
done
```

```
done
```

```
# 9) We also would like to allow access to our web server:
```

```
for OURIP in ${SERVER_IPS}; do  
    ${FWIN} -p tcp -d ${OURIP} --dport 80 ${OK}  
    ${FWIN} -p tcp -d ${OURIP} --dport 443 ${OK}  
done
```

```
10) people are still crazy enough to use ftp
```

```
for OURIP in ${SERVER_IPS}; do  
    for PORT in 20 21; do  
        ${FWIN} -p tcp -d ${OURIP} --dport ${PORT} ${OK}  
        ${FWIN} -p tcp --sport ${PORT} -d ${OURIP} --dport 1024: !" --syn ${OK}  
        ${FWIN} -p udp -d ${OURIP} --dport ${PORT} ${OK}  
        ${FWIN} -p udp --sport ${PORT} -d ${OURIP} --dport 1024: ${OK}  
    done  
done
```

```
# allow answers on high ports
```

```
${FWIN} -p tcp -m tcp --dport 1024:65535 ! --tcp-flags SYN,RST,ACK SYN ${OK}  
${FWIN} -p udp -m udp --dport 1024:65535 ${OK}
```

```
# Everything else is denied by default - policy is DROP.
```

```
# OUTPUT
```

```
# 1) Loopback packets.
```

```
${FWOUT} -o lo ${OK}  
${FWOUT} -s 127.0.0.0/8 ${NO}
```

```
# 2) We allow all outgoing traffic:
```

```
for OURIP in ${SERVER_IPS}; do  
    ${FWOUT} -s ${OURIP} ${OK}  
done
```

```
::
```

```
stop)
```

```
# turn off the firewall, flush all rules  
echo "Flushing rulesets.."
```

```
stop INPUT  
stop OUTPUT  
stop FORWARD
```

```
;;
status)
    # display the current status - both firewall rules and masquerading
    # connections

    # list rules. -n avoids DNS lookups
    $IPTABLES -nL

;;

*)
    echo "Usage: firewall {start|stop|restart|status}"
    exit 1
esac

exit 0
```

Update: [CODE] tag added

---