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

        # 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

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by Vasily Tarasov on Fri, 06 Oct 2006 07:25:33 GMT
View Forum Message <> Reply to Message

Hello,

Thanks for the script - now we can give it as an example for newbies!
You sad that it doesn't permit ftp access. For me it's wrong: script allows ftp access. Maybe the reason is in a missprint in your script:

```
  # 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                                    <<<<  NO SIGN
OF COMMENT (#) IN THE BEGINING!
        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}

Thanks again!

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by whatever on Fri, 06 Oct 2006 07:43:07 GMT
View Forum Message <> Reply to Message

After # that too it don't work.
Problem is when we connect VPS it stops after connection goes to passive mode.
When I stop the firewall it works.
Can you test on your server and let me know.
I am running pureftpd
Thanks

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by Vasily Tarasov on Fri, 06 Oct 2006 08:56:21 GMT
View Forum Message <> Reply to Message

Well, of course passive mode doesn't work!
In passive mode server opens additional unpriviled port (>1024) and sends its number to client.
Client should connect to this port, but your iptables rules DROP these packets!

2024 - is just an example.

HTH,
vass.

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by whatever on Fri, 06 Oct 2006 09:47:26 GMT
View Forum Message <> Reply to Message

Do we have to enable the passive mode in the pureftpd config file too?
The firewall rules drop anything above 1024. In pureftpd config file # PassivePortRange

30000 50000
How do I enable this in firewall rules for port 20-21 as anything above 1024 is dropped

This rule is correct?

```
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 30000:40000 "!" --syn ${OK}
  ${FWIN} -p udp -d ${OURIP} --dport ${PORT} ${OK}
  ${FWIN} -p udp --sport ${PORT} -d ${OURIP} --dport 30000:40000 ${OK}
 done
done
```

Thanks

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by Valmont on Fri, 06 Oct 2006 09:53:14 GMT
View Forum Message <> Reply to Message

ip_conntrack,ip_conntrack_ftp?

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by Vasily Tarasov on Fri, 06 Oct 2006 10:08:58 GMT
View Forum Message <> Reply to Message

No!
You should make the following changes:

```
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 tcp -d ${OURIP} --dport 1024: ${OK}
   ${FWIN} -p udp -d ${OURIP} --dport ${PORT} ${OK}
-   ${FWIN} -p udp --sport ${PORT} -d ${OURIP} --dport 1024: ${OK}
+    ${FWIN} -p udp -d ${OURIP} --dport 1024: ${OK}
  done
done
```

This helps for me.
vass.

Subject: Re: Firewall rule don't allow ftp while port 21 is open
Posted by whatever on Fri, 06 Oct 2006 17:14:29 GMT
View Forum Message <> Reply to Message

Thank you Vass. It works like anything