

Forum:[Hack Forums](#)

Thread: [Are these iptables rules enough for a web server?](#)

jasonnix - January 21, 2024, 11:12 pm

Hello,

I have a server running Apache, Tor (Port 9050) and OpenVPN (Port 2024). Are the following iptables rules good and sufficient?

```
Code -P INPUT DROP
-P OUTPUT ACCEPT
-P FORWARD DROP
```

```
-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
```

```
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A INPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
-A INPUT -p tcp -m state --state NEW -m recent --update --seconds 60 --hitcount 20 -j DROP
-A INPUT -p tcp -m state --state NEW -m recent --set -j ACCEPT
```

```
-A INPUT -p udp -m udp --dport 2024 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 9050 -j ACCEPT
```

```
-A INPUT -s IP -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
```

```
-A INPUT -s IP -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
-A INPUT -s IP -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
-A INPUT -p tcp --dport 443 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

Regarding the web server I found the following rules and I have two questions:

```
Code # Allow incoming HTTP
```

```
-A INPUT -s IP -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

```
# Allow incoming HTTPS
```

```
-A INPUT -s IP -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

1- Why OUTPUT?

2- When you want to use HTTPS, is port 80 necessary?

Thank you.

Bastille - January 22, 2024, 12:55 am

Hey buddy,

Code -P OUTPUT ACCEPT> Means that every traffic is allowed to go out from your server. The problem is if someone get access to your server, he's able to initiate any request from it, for example : downloading a payload or something else. I would suggest you to allow OUTPUT only for the necessary protocols

Code -A INPUT -s IP -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT> You need to change the IP by the value of an IP you allow to access through SSH

Code -A INPUT -s IP -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
-A INPUT -s IP -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT> You need to configure the IP values if you want to restrict the access of your server through HTTP and HTTPS to one or more IP addresses.

2- When you want to use HTTPS, is port 80 necessary?
No

jasonnix - January 22, 2024, 3:06 am

(Jan 22, 2024 01:55 AM)Yseurk Wrote: [\[CITE\]](#) Hey buddy,

Code -P OUTPUT ACCEPT> Means that every traffic is allowed to go out from your server. The problem is if someone get access to your server, he's able to initiate any request from it, for example : downloading a payload or something else. I would suggest you to allow OUTPUT only for the necessary protocols

Code -A INPUT -s IP -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT> You need to change the IP by the value of an IP you allow to access through SSH

Code -A INPUT -s IP -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
-A INPUT -s IP -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT> You need to configure the IP values if you want to restrict the access of your server through HTTP and HTTPS to one or more IP addresses.

2- When you want to use HTTPS, is port 80 necessary?
No

Hi,

Thank you so much for your reply.

I know, I just used IP to hide the server's real IP address. Thanks for the OUTPUT tip, but I have Tor and OpenVPN on this server. Shouldn't the OUTPUT value be ACCEPT?

Bastille - January 22, 2024, 3:30 am

If you accept OUTPUT to any protocol and any IP address it's a vulnerability in case your web server is accessed by someone not legitimate. You should add some rules to filter what is allowed to go outside.

I've never setup a Tor related server, I usually configure firewalls (Fortinet, Palo Alto) but for a web server I assume that it works like that :

- Connections are initiated by users, that means if the connection comes from outside (INPUT) and is allowed, the server is allowed to reply (so we don't care about the OUTPUT)

- The OUTPUT rules are important if the connection/request are initiated BY THE SERVER. If the server has to initiate a connection (if you have back-end stuff, scheduled tasks and so on for example), you allow OUTPUT only on IP addresses you need, and protocols you need.

Usual allowed protocols for OUTPUT are :

- DNS (to update his database for example)
- NTP (to be up to date)
- HTTP
- HTTPS
- DHCP (if some IP settings are dynamic, but you usually configure it static)

and, if needed, depending on your usage, other protocols such as SNMP (162) if you monitor your server, SSH (22) if you really need to use SSH FROM YOUR SERVER to connect to another machine, etc

It's not an obligation, but it's a security enhancement

jasonnix - January 23, 2024, 10:04 pm

(Jan 22, 2024 04:30 AM)Yseurk Wrote: [CITE](#) If you accept OUTPUT to any protocol and any IP address it's a vulnerability in case your web server is accessed by someone not legitimate. You should add some rules to filter what is allowed to go outside.

I've never setup a Tor related server, I usually configure firewalls (Fortinet, Palo Alto) but for a web server I assume that it works like that :

- Connections are initiated by users, that means if the connection comes from outside (INPUT) and is allowed, the server is allowed to reply (so we don't care about the OUTPUT)
- The OUTPUT rules are important if the connection/request are initiated BY THE SERVER. If the server has to initiate a connection (if you have back-end stuff, scheduled tasks and so on for example), you allow OUTPUT only on IP addresses you need, and protocols you need.

Usual allowed protocols for OUTPUT are :

- DNS (to update his database for example)
- NTP (to be up to date)
- HTTP
- HTTPS
- DHCP (if some IP settings are dynamic, but you usually configure it static)

and, if needed, depending on your usage, other protocols such as SNMP (162) if you monitor your server, SSH (22) if you really need to use SSH FROM YOUR SERVER to connect to another machine, etc

It's not an obligation, but it's a security enhancement

Hi Bro,

Thanks again.

So if I use :OUTPUT DROP, then the following iptables rules are required for both input and output:

Code # Allow incoming HTTP

```
-A INPUT -s IP -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

Allow incoming HTTPS

```
-A INPUT -s IP -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

This is one of the reasons why the above commands are written for both input and output. Am I

right?