

Cloudflare Error 521: Proxmox Host and VM with Web Servers Are Down

Cloudflare Error 521: web server is down

Things to check:

- Check Error Logs
- Check All Services is running (Nginx, PHP-fpm, mysql)
- Check Firewall Forwarding Rules
- Check Cloudflare DNS Records
- Check Domain Expired

My Host infrastructure:

- Host Proxmox pve1
 - pve1 has firewall rules and Route masquerading NAT which port forwarding port 80 , 443 to the VM 100
 - The host proxmox has VM 100
 - VM 100 has firewall rules respond back to the host pve1

Problem 1: Proxmox Host Firewall Rules are Gone after Restart

The problem here is when we restart the host proxmox pve1 , all firewall rules has been gone.

Solution:

ip address of VM 100: 192.168.xxx.3

Port Forwarding

Forward Port For HTTP (Port 80)

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.xxx.3:80
sudo iptables -A FORWARD -p tcp -d 192.168.xxx.3 --dport 80 -j ACCEPT
```

Forward Port for HTTPS (port 443)

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 192.168.xxx.3:443
sudo iptables -A FORWARD -p tcp -d 192.168.xxx.3 --dport 443 -j ACCEPT
```

Allow Traffic on Host:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

Enable IP Forwarding:

To make this change persistent across reboots, edit `/etc/sysctl.conf` and ensure the following line is uncommented:

```
net.ipv4.ip_forward = 1
```

apply the changes with

```
sudo sysctl -p
```

Verify the Configuration

To check if the port forwarding is working, you can:

Try accessing the web service on the host IP (e.g., `http://public.ip.address` or `https://your.public.ip.address`).

Ensure the VM's web service is running and listening on the correct ports (80 for HTTP and 443 for HTTPS).

Save the iptables Rules

If everything works as expected, save your `iptables` rules to ensure they persist across reboots.

For most Linux distributions, you can save the rules with:

```
sudo iptables-save > /etc/iptables/rules.v4
```

Check again, to see ports are being forwarded to the right vm ip addresses

List all `iptables` rules including NAT (Network Address Translation)

```
sudo iptables -t nat -L -n -v --line-numbers
```

```
root@pve1:/# sudo iptables -t nat -L -n -v --line-numbers
Chain PREROUTING (policy ACCEPT 5039 packets, 332K bytes)
num  pkts bytes target    prot opt in     out     source    destination
1    18749 1124K DNAT      6    --  *      *       0.0.0.0/0  0.0.0.0/0      tcp dpt:80 to:192.168.8.80
2     7077  425K DNAT      6    --  *      *       0.0.0.0/0  0.0.0.0/0      tcp dpt:443 to:192.168.8.443

Chain INPUT (policy ACCEPT 241 packets, 35510 bytes)
num  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 5 packets, 380 bytes)
num  pkts bytes target    prot opt in     out     source    destination

Chain POSTROUTING (policy ACCEPT 25824 packets, 1549K bytes)
num  pkts bytes target    prot opt in     out     source    destination
1    5211  327K MASQUERADE 0    --  *      vmbr0   192.168.192.0/18  0.0.0.0/0
2         0      0 MASQUERADE 0    --  *      vmbr0   192.168.192.0/18  0.0.0.0/0
```

Check Forward Rules

```
sudo iptables -L FORWARD -n -v --line-numbers
```

```
root@pve1:/# sudo iptables -L FORWARD -n -v --line-numbers
Chain FORWARD (policy ACCEPT 254K packets, 707M bytes)
num  pkts bytes target    prot opt in     out     source    destination
1    284K  40M ACCEPT     6    --  *      *       0.0.0.0/0  192.168.8.80    tcp dpt:80
2   10318 619K ACCEPT     6    --  *      *       0.0.0.0/0  192.168.8.443  tcp dpt:443
```

Save the current iptables rules

```
sudo iptables-save > /etc/iptables/rules.v4
```

```
sudo apt install iptables-persistent
```

```
sudo netfilter-persistent save
```

```
sudo systemctl enable netfilter-persistent
```

Revision #6

Created 14 May 2025 11:24:46 by Son.KyLuat

Updated 14 May 2025 14:59:51 by Son.KyLuat