# Web Server

Our front-facing public webserver. You're literally connected to this server right now, as you're on our wiki.

## Host Information

- IP: 128.205.44.157
- IP: 192.168.0.21 (Red Team Network)
- Reverse DNS: net-def.cse.buffalo.edu
- vCenter Cluster: MAIN
- vCenter Datastore: cdr-iscsi1

## Access Control

Access to this server is controlled via our central authentication server.

## Firewall Rules

As this machine is dual-homed, we have additional firewall rules on it. Below is the (saved) IPTables rules.

/etc/iptables/rules.v4

```
# Generated by iptables-save v1.4.21 on Mon Feb 19 17:37:45 2018
*filter
:INPUT DROP [15:1067]
:FORWARD ACCEPT [0:0]
:OUTPUT DROP [0:0]
:fail2ban-ssh - [0:0]
-A INPUT -p tcp -m multiport --dports 22 -j fail2ban-ssh
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -d 128.205.32.55/32 -p tcp -m tcp --dport 25 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

```
-A OUTPUT -d 192.168.0.50/32 -j ACCEPT
-A OUTPUT -d 128.205.44.172/32 -p udp -m udp --dport 1514 -j ACCEPT
-A OUTPUT -d 128.205.44.172/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 192.168.15.200/32 -p tcp -m tcp --dport 8080 -j ACCEPT
-A OUTPUT -d 192.168.13.138/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A fail2ban-ssh -j RETURN
COMMIT
# Completed on Mon Feb 19 17:37:45 2018
```

## Notes

fail2ban is installed, protecting against SSH bruteforce attacks. Don't mess up a login multiple times, as your IP will be banned.