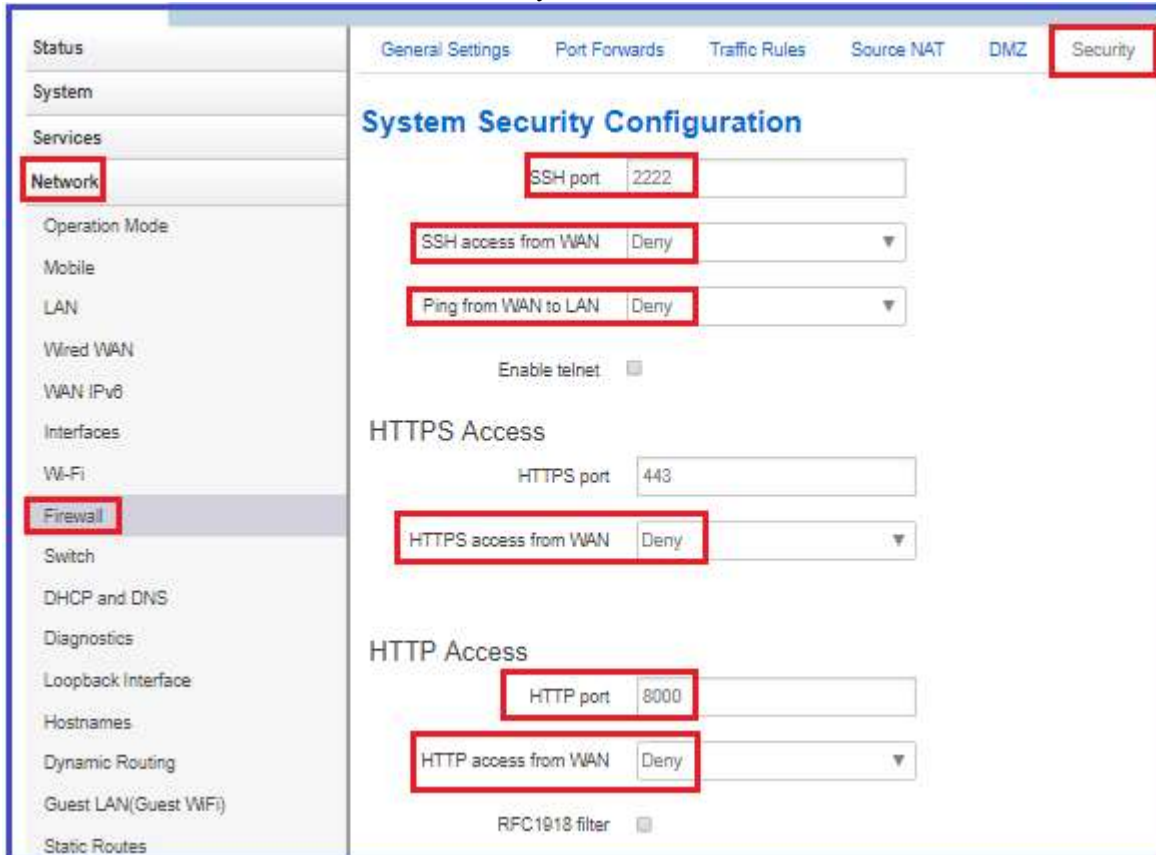


## How to restrict remote access to the CM685V router to pre-defined IP addresses

**Note:** In the Security settings provided below, we have changed default SSH port(22) to 2222, blocked SSH access from WAN, blocked HTTPS access from WAN, changed default HTTP port(80) to 8000 and blocked HTTP access from WAN for security purposes. We restricted remote access to pre-defined Public WAN IP addresses as set on the Whitelist.


### 1. Go to Network -> Firewall -> Security



The screenshot shows the 'System Security Configuration' page. The left sidebar has 'Network' and 'Firewall' highlighted. The main content area includes the following settings:

- SSH port:** 2222
- SSH access from WAN:** Deny
- Ping from WAN to LAN:** Deny
- Enable telnet:**
- HTTPS Access:**
  - HTTPS port:** 443
  - HTTPS access from WAN:** Deny
- HTTP Access:**
  - HTTP port:** 8000
  - HTTP access from WAN:** Deny
- RFC1918 filter:**

### 2. Enable Whitelist and enter Public WAN IP addresses that are allowed for remote access.



The screenshot shows the 'Access Whitelist' page. The left sidebar has 'Network' and 'Firewall' highlighted. The main content area includes the following settings:

- Enable:**
- IP address:** 101.187.145.165
- IP address:** 123.145.156.123