



# TickFlow Capital

## VPS Security Checklist

20-Point Audit for Trading Infrastructure

v1.0 – April 2026

### Audit Information

Audit Date: \_\_\_\_\_

Auditor Name: \_\_\_\_\_

VPS IP/Hostname: \_\_\_\_\_

Instructions: Mark each item as (Complete), (Partial), or (Missing)

### 20-Point Security Checklist

#### SSH Configuration (8 items)

#	Category	Item	Status
1	SSH	Disable password authentication ( <code>PasswordAuthentication no</code> )	<input type="checkbox"/>
2	SSH	Enable key-based authentication ( <code>PubkeyAuthentication yes</code> )	<input type="checkbox"/>
3	SSH	Change default port (22 → custom, e.g., 22222)	<input type="checkbox"/>
4	SSH	Disable root login ( <code>PermitRootLogin no</code> )	<input type="checkbox"/>

#	Category	Item	Status
5	SSH	Limit authentication attempts ( <code>MaxAuthTries 3</code> )	<input type="checkbox"/>
6	SSH	Set idle timeout ( <code>ClientAliveInterval 300,</code> <code>ClientAliveCountMax 2</code> )	<input type="checkbox"/>
7	SSH	Verify authorized_keys permissions ( <code>chmod 600</code> )	<input type="checkbox"/>
8	SSH	Test config before closing current session	<input type="checkbox"/>

## Fail2ban Configuration (2 items)

#	Category	Item	Status
9	fail2ban	Install fail2ban ( <code>sudo apt install fail2ban</code> )	<input type="checkbox"/>
10	fail2ban	Configure jail for custom SSH port	<input type="checkbox"/>

## UFW Firewall Configuration (3 items)

#	Category	Item	Status
11	UFW	Set default deny incoming ( <code>sudo ufw default deny incoming</code> )	<input type="checkbox"/>
12	UFW	Allow SSH only from your IP	<input type="checkbox"/>
13	UFW	Allow only necessary app ports (MT5, Grafana, etc.)	<input type="checkbox"/>

## Secrets Management (3 items)

#	Category	Item	Status
14	Secrets	Remove hardcoded keys from source code	<input type="checkbox"/>
15	Secrets	Use environment variables for API keys	<input type="checkbox"/>
16	Secrets	Set .env file permissions ( <code>chmod 600</code> )	<input type="checkbox"/>

## Docker Security (2 items)





#	Category	Item	Status
17	Docker	Run containers as non-root user ( <code>user: "1000:1000"</code> )	<input type="checkbox"/>
18	Docker	Pass secrets as environment variables (not volumes)	<input type="checkbox"/>

## Monitoring & Safety (2 items)

#	Category	Item	Status
19	Monitoring	Set up Prometheus + Grafana	<input type="checkbox"/>
20	Kill Switch	Implement Redis-based pause/halt/kill mechanism	<input type="checkbox"/>

## Scoring & Assessment

### Security Rating Scale

Score Range	Rating	Status	Action Required
0–10	 <b>Basic</b>	High Risk	Immediate improvements required
11–15	 <b>Moderate</b>	Elevated Risk	Review missing items, schedule follow-up
16–18	 <b>Good</b>	Acceptable	Production-ready for most retail traders
19–20	 <b>Excellent</b>	Low Risk	Institutional-grade security

**Your Score:** \_\_\_\_ / 20

**Recommended Rating:** \_\_\_\_

### Priority Fixes (Score < 10)

If your score is below 10, prioritize these items immediately:

1. **SSH hardening** – Disable root login + password auth (items 1, 2, 4)

2. **fail2ban installation** – Protect against brute-force (item 9)
  3. **UFW firewall** – Default deny + restrict ports (items 11–13)
  4. **Secrets management** – Remove hardcoded keys (items 14–16)
- 

## Next Steps

- Schedule follow-up audit in **30 days**
  - Subscribe to security advisories (CVE feeds):
    - Ubuntu Security Notices: <https://ubuntu.com/security/notices>
    - NIST NVD: <https://nvd.nist.gov>
  - Enable system log aggregation (Loki/ELK)
  - Test disaster recovery procedures quarterly
  - Document all changes in change log
- 

## Quarterly Review Checklist

Review Date	Score	Auditor	Notes
Q2 2026	_____	_____	_____
Q3 2026	_____	_____	_____
Q4 2026	_____	_____	_____

---



TickFlow Capital

**Website:** [tickflowcapital.com](https://tickflowcapital.com)

**Version:** v1.0 – April 2026

© 2026 Tickflow Capital Limited. All rights reserved.

**Disclaimer:** This guide is provided for educational purposes. Always test on a demo account first. The kill switch is a safety mechanism but is not a substitute for careful

risk management.