Advisory: Firewall Security

9 September 2026

TLP:CLEAR

Mitigating Risks from Firewall Credential Breaches

This advisory is relevant to all Samoan individuals, IT managers and organisations. This alert is intended to be understood by both general and technical audiences.

What is it?

Firewalls are the backbone of modern network security. Firewalls provide a network perimeter defence by blocking malicious traffic and monitoring the flow of network activity. Users, organisations and businesses in Samoa use firewalls to secure IT operations and monitor internal traffic to protect network data.

What is the issue?

Since firewalls are **fundamental for modern network security**, firewall configuration and management are essential. If the appropriate controls are not in place, users and organisations can expose themselves to inadvertent harm.

In particular, if administrative credentials are exposed and no compensating controls are in place, attackers could potentially have unfettered access to a system's network, internal operations and confidential data.

Samoan IT managers and firewall operators **need to be alert to the risk posed by potential credential breaches** and should act accordingly to protect their organisations.

If you manage a FortiGate device, you need to be **aware of the following incident and urgently implement the security advice.**

FortiBleed Data Breach *June 2026*

If you manage a Fortinet firewall, your details may have already been breached. In June, cybercriminals revealed that a significant portion of FortiGate firewall credentials had been stolen.

Fortinet released a swift advisory to instruct vendors to **ensure proper firewall configuration** and **robust identity management solutions.**

This is not **the fault of the firewall**. Even the most powerful software **needs a human hand.**

Over 70,000 administrator credentials were leaked, possibly affecting 900,00 users.

Users were concerned about flow-on malware attacks and malicious ingress.

How do I stay secure?

For IT managers, consider what devices you manage.

If you **manage a Fortinet firewall:**

1. **Urgently read** Fortinet's vulnerability advisory and implement the recommended controls.
2. Validate configuration status and MFA presence on administrator accounts.
3. Check the version status and upgrade to the latest version.

See *Appendix A: Fortinet Recommendations*

If not, **still apply core access principles.**

1. Consider reading Fortinet's vulnerability advisory.
2. Check the device model, software version and apply core access principles.
3. Contact SamCERT with any questions.

See *Appendix B: Access Management Principles*

If you have been affected by malware or have experienced a cyber incident, contact SamCERT on:

www.samcert.gov.ws/report-incident

samcert@mcit.gov.ws

+685 26 117

TLP:CLEAR

Advisory: Firewall Security

9 September 2026

TLP:CLEAR

Appendix A: Fortinet Advisory

Appendix A is a briefing note, summarising the key recommendations of the Fortinet *Analysis of Reported Credential Compromise of FortiGate Devices* advisory.

Please refer to the above Fortinet advisory for detailed recommendations and technical specifications.

Situational Analysis

Fortinet's analysis indicates that the reported "FortiBleed" activity was not caused by a new vulnerability.

Instead, threat actors were reportedly exploiting previously compromised credentials and using brute-force attacks against devices that had weak password practices and lacked multi-factor authentication (MFA).

Recommended Actions

1. **Terminate all administrator and VPN sessions and reset credentials**. Terminate all active administrative sessions. Reset all Fortinet VPN and administrative passwords, especially on internet-facing systems, and enforce strong password policies.

2. **Implement MFA on all administrator and VPN user accounts**.

3. **Upgrade to the latest versions of 7.4, 7.6, or 8.0.** These versions support PBKDF2 hashing of administrator credentials. Follow the guidance to remove older legacy password settings via set login-lockout-upon-weaker-encryption.

4. **Validate configuration.** Review firewall and VPN users, and other configurations, for unauthorised changes. Preferably compare to a known good configuration. Pay particular attention to the addition of unrecognised accounts, such as “forticloud, fortiuser, fortinet-support, fortinet-tech-support,” etc.

5. **Check your logs.** Look for unexpected administrator access from an unknown IP address, and review domain controller logs for lateral movement, unusual access, suspicious accounts or unauthorised configuration changes.

6. **Reduce your attack surface and lock down management access.** Restrict external management of your devices via trusted hosts (good), a local-in policy (better), or remove internet administration altogether (best).

These recommendations provide an abridged summary of Fortinet’s full recommendations. Please refer to the attached resources for official configuration and hardening instructions and consult vendor recommendations directly for further security protocols.

Fortinet’s FortiBleed Advisory Fortinet’s Configuration Guide

If you have been affected by malware or have experienced a cyber incident, contact SamCERT on:

www.samcert.gov.ws/report-incident samcert@mcit.gov.ws +685 26 117