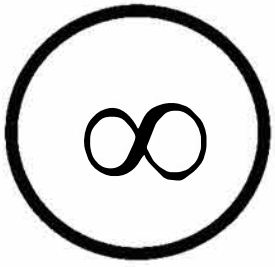


iNFINITY

Cybersecurity Audit Report

June 3rd, 2025

Table of Contents

Executive Summary

The following cybersecurity audit of Infinity assesses its use of the SonicWall NSa (Network Security Appliance) Firewall, one of the next generation firewalls designed for business and organizations in need of advanced, high performance security solutions.

Improved intrusion detection, anti-spyware, handling of large volumes of traffic, and cloud-based management are just some of its features.

I reviewed security requirements 8.1.6. through 8.1.8 -- compiled from the Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1 -- to assess the SonicWall NSa's controls regarding identifying and authenticating access to system components.

Key Findings

- Misconfiguration of access controls:
    - The lockout attempt setting is nearly twice the amount required by the standard.
    - While log out after inactivity is set to 30 minutes, the lockout time itself is set only to 5.
    - The duration for log out after inactivity is twice what it should be.

Recommendations

To address these issues, I advised Infinity to routinely review its access controls to protect sensitive data, ensure controls are properly configured and scaled down or up to meet compliance.

Objective, Scope, and Methodology

Objective

Determining Infinity's PCI DSS compliance and the effectiveness of its use of the SonicWall NSa Firewall is the objective of this audit. While the software offers several robust measures to aid in security, lax settings could render them redundant.

Controls tested aid in identifying and authenticating access to system components, protecting sensitive data and ensuring accountability among trusted users.

Scope

While the scope of this assessment only focused on controls 8.1.6 through 8.1.8 taken directly from the PCI DSS framework, these requirements prove crucial in sustain the integrity of critical system components and cardholder data.

Methodology

To assess the effectiveness of Infinity's use of the SonicWall NSa Firewall and compliance with the Payment Card Industry Data Security Standard, I reviewed controls 8.1.6 through 8.1.8.

See a breakdown of the requirements in the figure below:

PCI DSS Requirements 8.1.6 -- 8.1.8	
Control ID	**Defined**
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

Findings

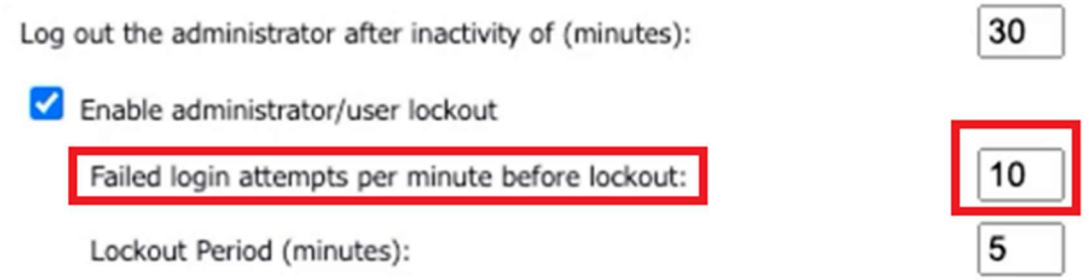
Infinity's use of the SonicWall NSa (Network Security Appliance) Firewall was found not complaint based on the following criteria:

Requirement 8.1.6

Limit repeated access attempts by locking out the user ID after not more than six attempts.

As shown in the figure below, their lockout attempt setting is nearly twice the amount required by the standard. By restricting the number of login attempts, systems can protect user accounts, send notifications to trusted parties after repeated login failures, and halt automated attacks.

Figure 2: Failed Login Attempts Per Minute

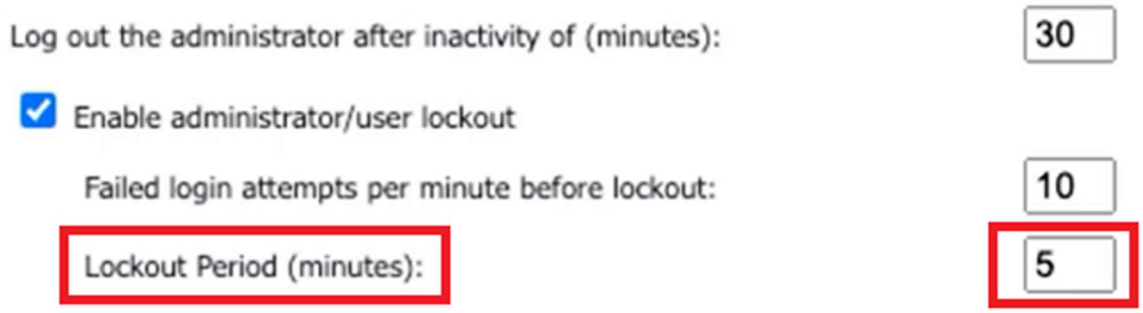


Requirement 8.1.7

Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

While Infinity's log out after inactivity is set to 30 minutes, the lockout itself is set only to 5. This could result in lack of accountability, weakened defenses -- especially from repeated attacks, and unauthorize access to sensitive data.

Figure 3: Lockout Duration



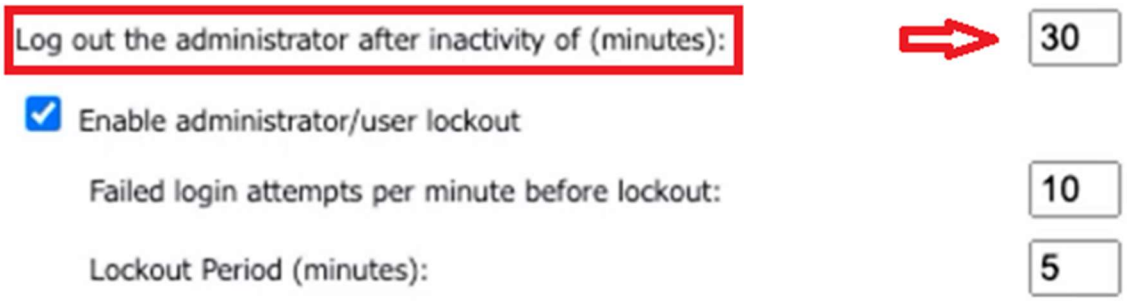
Requirement 8.1.8

If a session has been idle for more than 15 minutes, require the user to re-authenticate to re--activate the terminal or session.

As seen below, the duration for log out after inactivity is twice what it should be.

Re--authenticating ensures the user's identity is who they say they are and is authorized to access certain information and helps protect sensitive data if the account is seized.

Figure 4: Inactivity Logout Duration



While keeping the current settings may be more convenient, especially when pressed for time, making the necessary changes ensures yet another layer of protection from relentless hackers utilizing various methods. For example, a hacker attempting a brute force attack or dictionary could correctly guess user passwords in just a few minutes.

As everyday technology advances, the slightest misconfiguration -- no matter how inconsequential it may seem -- could lead to a disastrous data breach.

Recommendations

To address any area of non-compliance and to boost security, Infinity should:

1. Routinely review its access controls to protect sensitive data, reduce risks of unauthorized access, and respond to an incident in a timely manner.

2. Ensure controls are properly configured to preserve overall system and account integrity and reduce the flow of productivity.

3. Change access control settings to meet PCI DSS compliance. This includes:

    - Lowering failed login attempts per minute before lockout time from ten to six minutes.
    - Increasing lockout duration time from five to thirty minutes.
    - Decreasing inactivity logout duration from thirty to fifteen minutes.

The importance of following the security standards and implementing the suggested changes outlined in the assessment cannot be stressed enough. I trust that this audit helped you zero in on potential risks and that you will apply the proper changes as soon as possible.

If you have any questions, I'm available at the following address: jkinfluker@gmail.com

Thank you,

J. Fluker

GRC Analyst