RAPIDFIRE

by H.I.C. CYBERSECURITY

Firewall Audits Done Right

What Will A Firewall Audit Help Me Do?

Obtain Configuration Oversight

Firewalls configuration changes are often made on a daily or weekly basis. Many changes introduce unintended risk through configuration mistakes, overly permissive rules, temporary rules that do not automatically expire, and many others.

Keep Up With Best Practices by the Manufacturer

Best practice recommendations evolve constantly and often are the exact opposite of the old or original recommendations because new functionality removes limitations that the original recommendations were based on.

Take Advantage of New Features

Manufacturers are constantly adding better feature sets and improving existing functionality, however, they are typically disabled by default and require a manual change to enable. Regular audits help identify gaps between available functionality and currently configured functionality.

Stay Current with your Hardware and Firmware

As Firewall hardware and software become outdated you must identify firmware and hardware that is going end of life to avoid exposure to unsupported software that could contain vulnerabilities that are not actively being patched.

Meet Compliance Requirements

Most compliance standards have specific requirements for firewall configurations and feature sets.

H.I.C.
CYBERSECURITY

To Learn More Please Contact:

Vanessa Lardiere
SVP of Sales
(917) 301-9172
VLardiere@hiccybersecurity.com

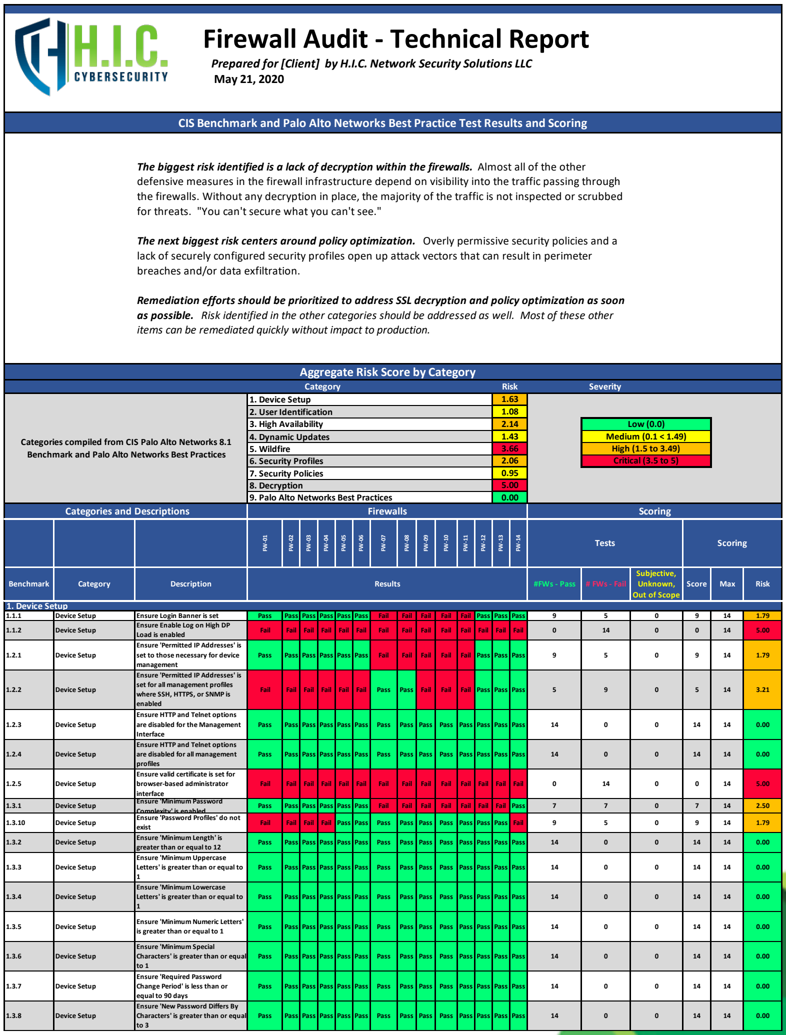
RAPID FIRE

by H.I.C. CYBERSECURITY

Firewall Audits Done Right

What Will My Firewall Audit Look Like?

A Multi-Page Technical Report similar to the one below
as well as a written Executive Report



Firewall Audit - Technical Report

Prepared for [Client] by H.I.C. Network Security Solutions LLC
May 21, 2020

CIS Benchmark and Palo Alto Networks Best Practice Test Results and Scoring

The biggest risk identified is a lack of decryption within the firewalls. Almost all of the other defensive measures in the firewall infrastructure depend on visibility into the traffic passing through the firewalls. Without any decryption in place, the majority of the traffic is not inspected or scrubbed for threats. "You can't secure what you can't see."

The next biggest risk centers around policy optimization. *Overly permissive security policies and a lack of securely configured security profiles open up attack vectors that can result in perimeter breaches and/or data exfiltration.*

Remediation efforts should be prioritized to address SSL decryption and policy optimization as soon as possible. *Risk identified in the other categories should be addressed as well. Most of these other items can be remediated quickly without impact to production.*

Aggregate Risk Score by Category

	Category	Risk	Severity
Categories compiled from CIS Palo Alto Networks 8.1 Benchmark and Palo Alto Networks Best Practices	1. Device Setup	1.63	
	2. User Identification	1.08	
	3. High Availability	2.14	Low (0.0)
	4. Dynamic Updates	1.43	Medium (0.1 < 1.49)
	5. Wildfire	3.66	High (1.5 to 3.49)
	6. Security Profiles	2.06	Critical (3.5 to 5)
	7. Security Policies	0.95	
	8. Decryption	5.00	
	9. Palo Alto Networks Best Practices	0.00	

Categories and Descriptions			Firewalls														Scoring					
			FW-01	FW-02	FW-03	FW-04	FW-05	FW-06	FW-07	FW-08	FW-09	FW-10	FW-11	FW-12	FW-13	FW-14	Tests			Scoring		
Benchmark	Category	Description	Results														#FWs - Pass	# FWs - Fail	Subjective, Unknown, Out of Scope	Score	Max	Risk
1. Device Setup																						
1.1.1	Device Setup	Ensure Login Banner is set	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Pass	9	5	0	9	14	1.79
1.1.2	Device Setup	Ensure Enable Log on High DP Load is enabled	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	0	14	0	0	14	5.00
1.2.1	Device Setup	Ensure 'Permitted IP Addresses' is set to those necessary for device management	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Pass	9	5	0	9	14	1.79
1.2.2	Device Setup	Ensure 'Permitted IP Addresses' is set for all management profiles where SSH, HTTPS, or SNMP is enabled	Fail	Fail	Fail	Fail	Fail	Fail	Pass	Pass	Fail	Fail	Fail	Pass	Pass	Pass	5	9	0	5	14	3.21
1.2.3	Device Setup	Ensure HTTP and Telnet options are disabled for the Management Interface	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.2.4	Device Setup	Ensure HTTP and Telnet options are disabled for all management profiles	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.2.5	Device Setup	Ensure valid certificate is set for browser-based administrator interface	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Fail	0	14	0	0	14	5.00
1.3.1	Device Setup	Ensure 'Minimum Password Complexity' is enabled	Pass	Pass	Pass	Pass	Pass	Pass	Fail	Fail	Fail	Fail	Fail	Fail	Fail	Pass	7	7	0	7	14	2.50
1.3.10	Device Setup	Ensure 'Password Profiles' do not exist	Fail	Fail	Fail	Fail	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Fail	9	5	0	9	14	1.79
1.3.2	Device Setup	Ensure 'Minimum Length' is greater than or equal to 12	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.3	Device Setup	Ensure 'Minimum Uppercase Letters' is greater than or equal to 1	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.4	Device Setup	Ensure 'Minimum Lowercase Letters' is greater than or equal to 1	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.5	Device Setup	Ensure 'Minimum Numeric Letters' is greater than or equal to 1	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.6	Device Setup	Ensure 'Minimum Special Characters' is greater than or equal to 1	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.7	Device Setup	Ensure 'Required Password Change Period' is less than or equal to 90 days	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00
1.3.8	Device Setup	Ensure 'New Password Differs By Characters' is greater than or equal to 3	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	14	0	0	14	14	0.00

Available for:

Palo Alto Networks
Checkpoint
Cisco
Fortinet
Juniper Networks

Why Use H.I.C.?

We are experts in our field who understand firewalls inside and out. We can see missing items and simple nuances that result in misconfigurations or overly exposed rules and we can identify these quickly.

H.I.C.
CYBERSECURITY

To Learn More Please Contact:

Vanessa Lardiere
SVP of Sales
(917) 301-9172
VLardiere@hiccybersecurity.com