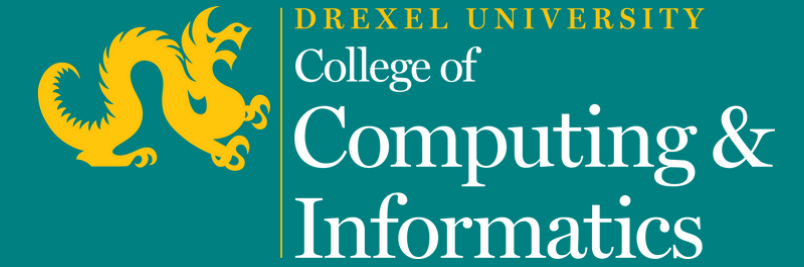




FireRate

Ryan Abraham, Wyman Li, Jason Ni, and Simon Wu
College of Computing Informatics (CCI) Drexel University

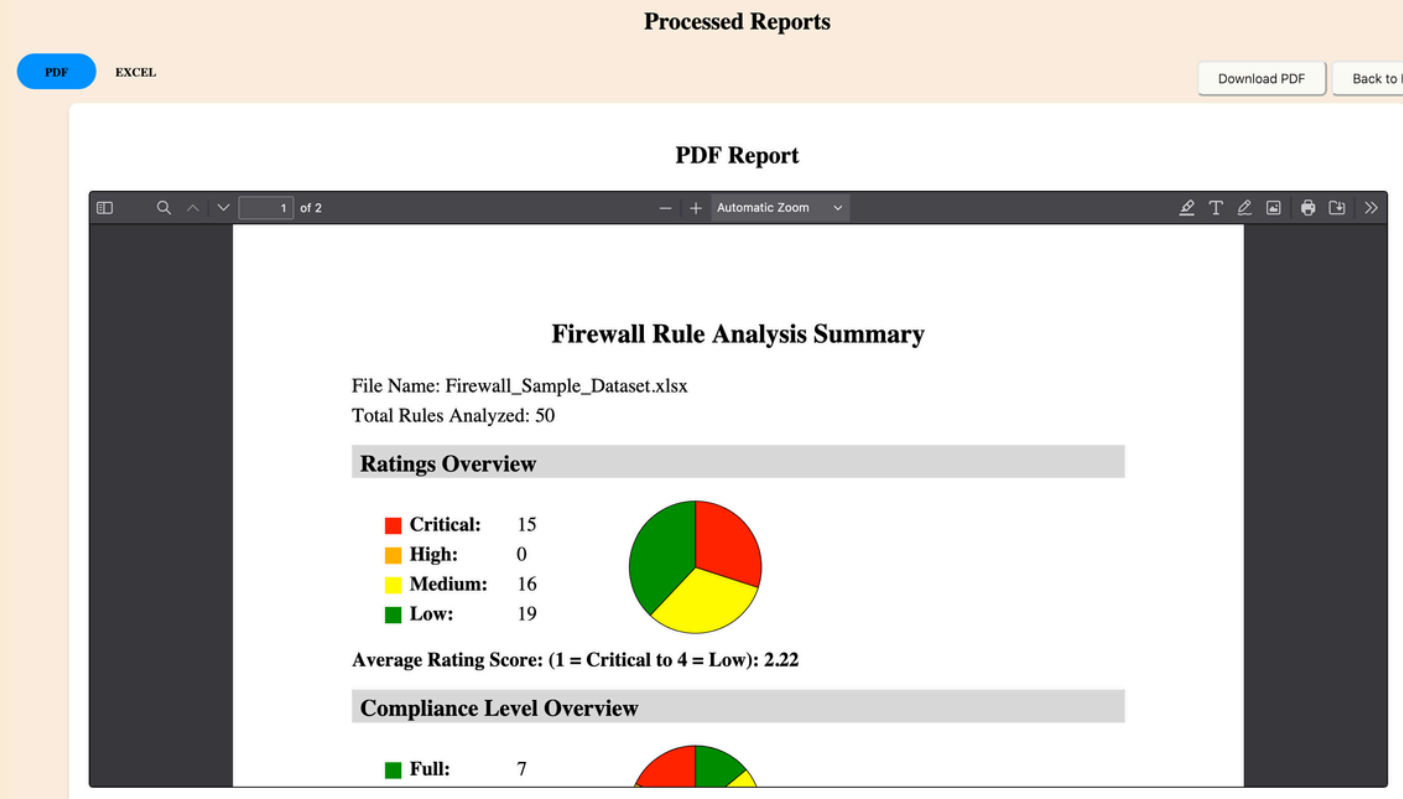


Purpose

- Our goal is to provide users the tools to educate and learn how to better secure their firewalls
- FireRate is a tool that assesses firewall rules through the lens of industry standard regulations like NIST.
- After uploading a formatted file of their firewall rules it will be rated and given recommendations

Technology

- FireRate is a locally-hosted web application.
- The website is designed primarily with HTML, CSS, and Javascript.
- Our script that is run through the Firewall Analyzer is created with Python.
- The FireRate team utilized Gitlab and a storyboard to deligate and faciliate task distribution.



Processed Reports

PDF EXCEL Download Excel Back to Home

Excel Report

Rule ID	Source IP	Destination IP	Port/ Protocol	Rule Type	Action	Compliance Framework	Logging	Description	Encryption	Score	Max Score	Compliance Level	Rating	Details	Recommendations
R1	any	192.168.79.33	ICMP	Access Rule	Deny	PCI DSS	Yes	Restrict ICMP traffic to prevent potential network mapping. Block unnecessary ICMP communications.	Yes	37 / 37	37	Full	Critical	Checked: IP scope with 'Deny' action and wide IP ranges (24/24). Checked: ICMP protocol with 'Deny' action (9/9). Checked: 'Deny' action with both logging and encryption (4/4).	Compliant
R2	any	any	443/TCP	Access Rule	Deny	SOX NIST	Yes	Comprehensive HTTPS traffic control. Block unauthorized external connections. Enforce strict SSL/TLS inspection.	Yes	37 / 37	37	Full	Critical	Checked: IP scope with 'Deny' action and wide IP ranges (24/24). Checked: TCP/UDP protocol with 'Deny' action (9/9). Checked: 'Deny' action with both logging and encryption (4/4).	Compliant
R3	any	any	445/TCP	Stateful Inspection	Deny	NIST PCI DSS	Yes	SMB protocol blocking. Prevent potential file-sharing vulnerabilities and unauthorized network access.	Yes	37 / 37	37	Full	Critical	Checked: IP scope with 'Deny' action and wide IP ranges (24/24). Checked: TCP/UDP protocol with 'Deny' action (9/9). Checked: 'Deny' action with both logging and encryption (4/4).	Compliant
R4	192.168.84.9	192.168.170.198	8080/TCP	NAT Rule	Allow	SOX HIPAA	Yes	Controlled internal application port access. Implement strict NAT.	No	24 / 41	41	Partial	Medium	Checked: IP scope further or use 'Deny' for broader scopes. Enforce both inspection.	Restrict IP ranges further or use 'Deny' for broader scopes. Enforce both inspection.

Scoring Rubric

- Our script is based off NIST SP-800-41 Guidelines on Firewalls and Firewall Policy

Processed Reports

- After analysis reports will be available in PDF and Excel format.
- The PDF will provide more digestible and easy to see information.
- The Excel file will provide more detailed and lengthy analysis

FireLearn

- The goal of FireLearn is to provide educational content so that users can learn more about securing their firewalls.
- Articles to teach users about different topics like what NIST is and their importance
- There is a quiz section that tests general knowledge of firewalls