Firewall Configuration Assessment Report

test_4

Date of Assessment: N/A

1. Report Summary

Overall Score: 33/65

Pros:

- Latest patches tested and applied from trusted sources.
- Latest patches tested and applied from trusted sources.
- Unused and critical ports are blocked according to policy.
- Echo requests and other unnecessary ICMP types are blocked.
- Only internal IP traffic is allowed to leave the network.
- Hot standby is configured for firewall redundancy.

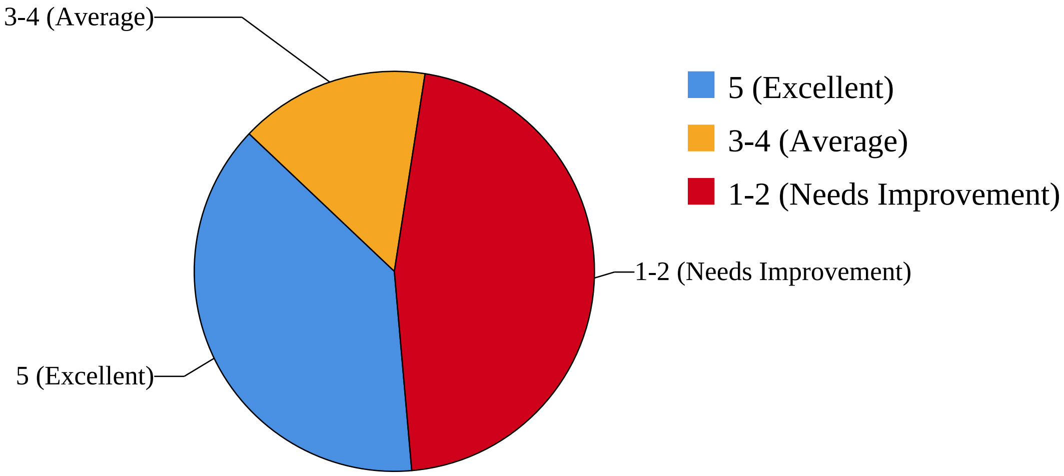
Cons:

- Long timeouts, no MAC or URL filtering, allowing harmful scripts.
- Logs disabled or ignored, missing critical attack indicators.
- Outdated software with unpatched vulnerabilities.
- Spoofed or illegal traffic is not filtered, posing security risks.
- Telnet or other insecure protocols are allowed.
- FTP is enabled within the internal network without safeguards.

2. Evaluation Details

Score detail

No.	Criteria	Score	Passed Steps/Total Steps
1	Review the rulesets order (in the following order)	3	3 / 5
2	Stateful inspection	1	1 / 4
3	Logging	0	0 / 2
4	Patches and updates	0	0 / 2
5	Vulnerability assessments/Testing	3	2 / 3
6	Compliance with security policy	5	1 / 1
7	Block spoofed, private, and illegal IPs	1	2 / 5
8	Port restrictions	5	2 / 2
9	Remote access	0	0 / 1
10	File transfers	0	0 / 1
11	ICMP	5	1 / 1
12	Egress filtering	5	2 / 2
13	Firewall redundancy	5	1 / 1



Failed steps

No.	Criterion	Failed Step
1	Review the rulesets order (in the following order)	Check user permit rules
1	Review the rulesets order (in the following order)	Check noise drops
2	Stateful inspection	Ensure harmful scripts like ActiveX, Java are blocked.
2	Stateful inspection	If using a URL filtering server, ensure definitions are correct.
2	Stateful inspection	Check MAC address filtering if used.
3	Logging	Ensure logging is enabled.
3	Logging	Periodically check logs for attack patterns.
4	Patches and updates	Ensure the firewall is updated to the latest patches.
4	Patches and updates	Check download sources (reliable websites or emails with digital signatures).
5	Vulnerability assessments/Testing	Check rulesets to prevent denial of service or vulnerabilities.
7	Block spoofed, private, and illegal IPs	+ Reserved addresses (240.0.0.0).
7	Block spoofed, private, and illegal IPs	+ Illegal addresses (0.0.0.0).
7	Block spoofed, private, and illegal IPs	+ UDP echo, ICMP broadcast (RFC 2644).
9	Remote access	Ensure SSH (port 22) is used instead of Telnet.
10	File transfers	Ensure the server supporting FTP is placed on a separate subnet from the internal network.

Scan Result

- The IP of external side: 192.168.1.1
- TCP:
  + Port 53 (open)
  + Port 80 (open)
  + Port 443 (open)
- UDP:
  + Port 53 (open)
- The ICMP rule on the external side of the firewall is: open

3. Recommendations

- There are 15 steps that are not passing. The admin should review these step and make change if it meet the requirement of the network.

Action Plan:

- Enable logging immediately and configure periodic log reviews.
- Replace insecure remote access protocols (e.g., Telnet) with secure options like SSH.
- Apply the latest firewall patches and ensure reliable download sources.
- Review and block the following illegal or spoofed IP addresses:
- ---+ Reserved addresses (240.0.0.0).
- ---+ Illegal addresses (0.0.0.0).
- ---+ UDP echo, ICMP broadcast (RFC 2644).
- Review and secure the following open ports:
- --- TCP: 53, 80, 443
- --- UDP: 53
- Block unnecessary ICMP traffic to reduce the risk of reconnaissance attacks.
- Optimize firewall ruleset order to minimize conflicts and improve performance:
- --- Check user permit rules
- --- Check noise drops
- Perform regular vulnerability assessments using tools like nmap to identify open ports and vulnerabilities:
- --- Check rulesets to prevent denial of service or vulnerabilities.
- Ensure periodic scans like the one completed on 28/11/2024 (17:30:19).

4. APPENDIX

The criterias

No.	Criteria	Definition
1	Review the rulesets order	Review the rulesets to ensure that they follow the order as follows: • anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) • User permit rules (e.g. allow HTTP to public webserver) • Management permit rules (e.g. SNMP traps to network management server) • Noise drops (e.g. discard OSPF and HSRP chatter) • Deny and Alert (alert systems administrator about traffic that is suspicious) • Deny and log (log remaining traffic for analysis) • Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order.
2	Stateful inspection	
3	Logging	
4	Patches and updates	
5	Vulnerability assessments/Testing	
6	Compliance with security policy	
7	Block spoofed, private, and illegal IPs	
8	Port restrictions	
9	Remote access	
10	File transfers	
11	ICMP	
12	Egress filtering	
13	Firewall redundancy	