Firewalls and Port Restrictions

Firewalls are an important part of cyber defense. You can set policies to manage firewalls to prevent unwanted behavior and reduce the risk of successful attack. On the other hand, a poorly protected firewall or bad configuration decisions can give threat actors an opportunity to gain access to private assets and resources.

Attackers search for vulnerable default settings and gaps or inconsistencies in firewall rule sets, routers, and switches, then use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

All firewalls, no matter how simple or small of a network, need to have their configurations managed. To properly manage network firewalls, you need to establish rules and policies, track changes, and monitor compliance logs. You should also implement and manage firewalls on end user devices.

Goals

1. Enable network scanning to look for port vulnerabilities (Level 1 maturity)
2. Enable firewall management on networks (Level 1 maturity)
3. Enable firewall management on end-user devices (Level 1 maturity)

Actions

For Firewalls and Port Restrictions, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

Manage firewalls on all servers and end-user devices.

1. Use free tools and services to conduct scans of your publicly-facing assets. This should include your website and any online portals you are responsible for that are used for elections purposes. Sign up for free vulnerability scanning by contacting CISA at vulnerability_info@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services."
2. Change default passwords for all applications, operating systems, routers, firewalls, wireless access points, printers, scanners, and other devices when adding them to the network.
3. Block all access by default, then allow-list traffic you want on the network.
4. Update firewall software automatically or on a set schedule. Stick to that schedule.
5. Limit administrative access to the firewalls to as few individuals as possible.
6. Review firewall rules on a set schedule. Stick to that schedule.

Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Implement a CIS Benchmark for firewall management that is appropriate for your environment.

Cost-Effective Tools

- Free vulnerability scanning from CISA. Contact vulnerability_info@cisa.dhs.gov with subject line "Requesting Cyber Hygiene Services."
- CIS Benchmark for firewall management: Secure configurations for more than a hundred of the most common software applications.

Mapping to CIS Controls and Safeguards

- 4.4: Implement and Manage a Firewall on Servers (Level 1 maturity)
- 4.5: Implement and Manage a Firewall on End-User Devices (Level 1 maturity)
- 13.9: Deploy Port-Level Access Control (Level 3 maturity)
- 13.10: Perform Application Layer Filtering (Level 3 maturity)

Mapping to CIS Handbook Best Practices

- 41, 42

‹ Previous
Managing Remote Connections

Next ›
Endpoint Protection

Made with Sphinx and @pradyunsg's Furo
Last updated on Oct 03, 2022