

Layered Defense and Firewall Selection for Small Businesses

Cybercrime cost small businesses **\$2.4 billion** in 2021, while CISA reported that small businesses were **three times** more likely to be targeted by cybercriminals than larger companies (CISA, 2023). Small businesses often have to make cybersecurity decisions without the staffing, budget, or specialized knowledge available to larger organizations. NIST notes that smaller businesses frequently operate with limited time, funding, and IT personnel, making practical and cost-effective cybersecurity particularly important (Eliot & Pillitteri, 2026). This creates a difficult question: how can a small organization build meaningful network security without creating an infrastructure that requires a dedicated security team to operate? One answer is layered defense, where multiple security controls work together rather than relying on a single protective measure. By examining how layered defense operates, comparing the strengths of several firewall technologies, and considering the needs of smaller organizations, a next-generation firewall can be evaluated as a practical foundation for network security.

Layered defense, also known as defense-in-depth, uses multiple defensive techniques so that the failure or bypass of one control does not leave the entire network unprotected. CISA states that no single defensive technique can prevent every attack and recommends a layered approach that creates multiple barriers while increasing opportunities to detect and respond to malicious activity (CISA, 2020). Building those layers requires more than installing security products. Organizations must identify important systems and information, evaluate risks, establish network boundaries, configure access controls, monitor activity, and periodically review security controls as conditions change. NIST similarly recommends that firewall solutions be selected, configured, tested, deployed, and continuously managed according to organizational security requirements (Scarfone & Hoffman, 2009). A firewall therefore represents one component of layered defense by controlling traffic between networks or systems with different security requirements.

Several firewall technologies can fill that role in different ways. **Stateful inspection firewalls** maintain information about active network connections and use that context when deciding whether traffic should be allowed (Cisco, 2026). **Proxy firewalls**, sometimes called application-level gateways, act as intermediaries between systems and can inspect application traffic before forwarding it to its destination (Cisco, 2026). **Web application firewalls** focus specifically on traffic involving web applications and inspect requests for malicious or unauthorized content (Cisco, 2026). **Unified threat management firewalls** combine stateful inspection with additional services such as intrusion prevention and antivirus protection, with an emphasis on simplified management (Cisco, 2026). Finally, **next-generation firewalls (NGFWs)** combine stateful inspection with application awareness, intrusion prevention, threat intelligence, and other advanced inspection capabilities (Cisco, 2026).

For a small organization, I would choose an NGFW as the primary network firewall. My reasoning is not that an NGFW makes every other security control unnecessary, but that it can place several useful capabilities under one administrative platform. Cisco notes that NGFW platforms can combine application control, intrusion prevention, threat detection, and centralized management, and some products are specifically designed to reduce administrative complexity for smaller IT organizations (Cisco, 2021; Cisco, 2026). In my view, that consolidation matters more to a small business than having the most specialized product for every individual security function. A company with one IT employee—or no dedicated IT employee at all—benefits when important protections can be configured and monitored from one place. The weakness is that an NGFW can still be misconfigured, may cost more than a basic firewall, and should not become the organization's only defense. For that reason, I would still combine it with endpoint firewalls, software updates, authentication controls, backups, and network segmentation.

Layered defense is ultimately about making security resilient rather than perfect. Smaller businesses may not be able to operate large collections of specialized security products, but they can still create multiple meaningful defensive layers. For that environment, an NGFW offers a strong balance between capability and manageability while leaving room for additional protections around it.

References

Cisco. (2021). *Cisco Secure Firewall Small Business Edition at-a-glance*. Cisco Systems.

Cisco. (2026). *What is a firewall?* Cisco Systems.

Cisco. (2026). *What is a next-generation firewall (NGFW)?* Cisco Systems.

Cybersecurity and Infrastructure Security Agency. (2020). *Technical approaches to uncovering and remediating malicious activity*.

Eliot, D., & Pillitteri, V. (2026). *Assessing security requirements for CUI: NIST SP 800-171Ar3 small business primer* (NIST SP 1352). National Institute of Standards and Technology.

Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). National Institute of Standards and Technology.