

Beyond Foundational Network Security



Your firewall is the foundation of your network security. But having just a firewall is no longer enough network security to protect your organization. These nine elements along with daily management of your firewall will ensure unwanted downtime and security threats.

1. Firewall/unified threat manager
2. Firewall configuration, reporting and updates
3. VPN tool management
4. Wireless protection
- 5.. Content filtering
6. Email & spam protection
7. Intrusion prevention
8. Mobile device management security
9. Security information and event management (SIEM)

1. Firewall/unified threat manager

Firewalls filter all information coming through your internet connection and block materials that are flagged by the firewall. Without it, your computers and data become accessible to anyone on the Internet, leaving your network open to hackers where valuable data can potentially get stolen, changed or lost. A firewall is the bare minimum of network security and is required by most compliance regulations.

2. Firewall configuration, reporting and updates

Firewalls require continual updates of the latest security patches. Without day-to-day management of your firewall, your employees and critical business assets are at risk from new threats. Hackers are always evolving, and that means your network security equipment should be updated at least daily to keep up with the latest security threats. Without regular updates, you may only be protected from yesterday's threats.

3. VPN Tool Management

A virtual private network (VPN) tool manager provides a secure internet connection to your remote users and the devices they use outside of the physical network perimeter. Often a VPN Tool manager is part of the managed firewall support from your IT provider.

4. Wireless Protection

Ensuring your wireless networks are secure and not accessible to unauthorized users is an important element of network security. Having separate wireless protection protocols for employee access and guest access are important first steps. But there are other key protocols as well, such as password management, enabling encryption on WiFi networks, and managing user settings of allowed/not allowed websites. Wireless protection is frequently part of a managed firewall service from your IT company



5. Content Filtering

Content filtering takes the protection of your firewall further by choosing specific subjects, titles, categories or words to restrict what types of material is accessible on your network. Content filtering can be used to block access to sites containing sexual material, violence, intolerance, drugs, illegal gambling, auction sites or any material deemed inappropriate in a professional work environment. Content filtering is typically handled by your firewall; your managed IT services provider can assist you with this.

6. Email & Spam Protection

Spammers have become sophisticated and now use advanced phishing schemes to collect personal and confidential material from your employees. Using email and spam protection services in conjunction with your managed firewall will block harmful email and email attachments from ever reaching your employees. Incoming traffic is also inspected for spyware and other known vulnerabilities such as worms and Trojans. Email and spam filtering is often an added on service to your managed IT Security solution.support from your IT provider.



7. Intrusion Prevention Service (IPS)

A firewall combined with an Intrusion Prevention Service provides the most complete protection against malicious network access attempts. The IPS sits between your firewall and the rest of your network and can stop suspicious traffic from penetrating the rest of the network. The IPS is used to defend against both internal and external attacks and adds improvements in security. Ask your computer service company about incorporating IPS into your firewall managed services.

8. Mobile Device Management (MDM)

If you're like most businesses, your staff members access company email from their smartphones, tablets and personal computers. Mobile device management creates a more secure environment for these devices being used by your employees – no matter where they are. MDM keeps your data safe if a device is stolen or lost, and it can also restrict or lock down access in the event of an employee being let go. MDM is usually part of or added onto a managed IT services solution.



9 .Security Information and Event Management (SIEM)

SIEM adds an additional security layer by providing real-time analysis of security alerts, and it logs security data and generates reports for compliance purposes. SIEMs can automate compliance reporting for PCI, HIPAA or any other regulatory agency. SIEMs require continual monitoring and optimization of tuning out false alarms, but a properly tuned SIEM will keep your organization safe and audit-ready. SIEM is typically an added-on security solution that your managed

Your Gulf Coast IT Partner



IT Support When You Need It.

These nine basic elements of network security for your organization set up a strong defense against malicious threats, human error or malice. If you find your organization questioning if you're currently using all these nine elements, or if you are curious if you "really" need them – then reach out to Gulfport, Mississippi's, AGJ Networks team today.

Why Choose AGJ's team of local IT experts?

- Experienced team of IT professionals
- Rapid response
- Honest, reliable, No "Geek Speak"

With Managed IT Services from AGJ Systems, you get:

- **24/7 monitoring** – get peace of mind knowing your systems are safe
- **Proactive maintenance** – we pinpoint and fix problems before they create downtime
- **Remote & overnight services** – so you experience fewer disruptions to your business
- **All-inclusive IT** – for predictable budgeting with flat-rate IT services that include hardware and software



Contact us for questions, information about our IT Management Services or a no-obligation IT consultation

Call us: 228-641-4688
Email: info@agjsystems.com

14257 Dedeaux Rd.
Gulfport, MS 39503

