Aishan Technologies

Best Practices for Hardening Sophos Firewalls

Prepared By: Hemanth Kurungat

Aishan Technologies

Introduction:

Aishan Technologies is dedicated to providing comprehensive solutions that ensure your network infrastructure is secure and resilient. This whitepaper details essential guidelines and best practices for strengthening ***Sophos firewalls***. By adhering to these recommendations, organizations can achieve robust protection against evolving cyber threats.

Problem Statement:

In today's digital landscape, cyber threats are increasingly sophisticated and persistent. Cybercriminals use advanced techniques such as phishing, ransomware, and zero-day exploits to infiltrate networks. Without proper firewall security measures, organizations face significant risks, including data breaches, malware infections, and other malicious activities. Additionally, incorrect or misconfigured security policies can lead to not only an increase in ransomware attacks but also a multitude of other security issues such as unauthorized access, data loss, and system vulnerabilities.

Impact of Cyber Threats:

Data Breaches: Unauthorized access to sensitive data can result in the theft of confidential information, including personal data, intellectual property, and financial records. Such breaches often lead to severe legal and regulatory consequences, especially with stringent data protection laws like GDPR and CCPA.

Malware Attacks: Malware, including viruses, trojans, and ransomware, can compromise network integrity, leading to the loss of crucial data, operational downtime, and the potential need for costly recovery efforts. Ransomware attacks, in particular, can encrypt critical data, rendering it inaccessible until a ransom is paid.

Reputation Damage: Cyber incidents can tarnish an organization's reputation, eroding customer trust and damaging brand loyalty. The negative publicity resulting from a security breach can have long-term repercussions on an organization's market position and profitability.

Operational Disruptions: Cyber attacks can disrupt normal business operations, causing significant downtime and affecting productivity. For instance, Distributed Denial of Service (DDoS) attacks can overwhelm network resources, making services unavailable to legitimate users.

Financial Losses: The financial implications of cyber attacks can be staggering. Costs associated with data breach notification, legal fees, regulatory fines, and remediation efforts

can amount to millions of dollars. Additionally, businesses may suffer from lost revenue due to operational disruptions and reputational damage.

Necessity for Stringent Security Practices:

To mitigate these risks, it is imperative for businesses to adopt stringent security practices to safeguard their network infrastructure and sensitive data. This involves a multi-layered security approach, including robust firewall configurations, regular security audits, employee training, and incident response planning.

Sophos Firewall's Role: Sophos Firewall offers advanced security features designed to protect organizations from sophisticated cyber threats. By implementing best practices for firewall management and configuration, businesses can enhance their security posture, ensuring comprehensive protection against malicious activities.

Why Aishan Technologies?: Aishan Technologies, with its expertise in cybersecurity and Sophos firewall solutions, is well-equipped to assist organizations in strengthening their network defenses. Our team of certified professionals provides tailored security solutions, continuous monitoring, and expert guidance to help businesses navigate the complex threat landscape.

Best Practices for Firewall Hardening

Keep Firmware Up to Date

Regularly updating your firewall firmware is crucial for maintaining security. Each Sophos Firewall OS update includes vital security enhancements, including the latest Sophos Firewall v21. Here are the best practices:

- **Frequent Checks**: Regularly check for firmware updates under *Backup & Firmware* > *Firmware*. At a minimum, this should be done monthly to ensure your firewall is protected against the latest vulnerabilities.
- **Deployment**: Deploy every update, including all maintenance releases (MRs), as these may include important security fixes that address newly discovered threats.
- **Scheduling**: Use Sophos Central to schedule updates during periods of minimal disruption, ensuring continuous protection without affecting operations. This allows updates to be installed during off-peak hours to minimize impact.

- **High Availability**: Consider a High-Availability (HA) deployment, which allows you to upgrade device firmware without any service interruption. This setup ensures that if one device fails, another can take over, maintaining network availability and security.
- **Community Engagement**: Stay informed about the latest firmware updates and security news via the Sophos Firewall Community. Engaging with the community can provide insights into emerging threats and best practices.

2. Limit Device Service Access

Limiting device service access is critical to reducing your attack surface:

- **Disable Non-Essential Services**: Ensure that non-essential services on the WAN interface, particularly HTTPS and SSH admin services, are disabled. This minimizes exposure to the internet, reducing the risk of unauthorized access.
- **Secure Remote Management**: For secure remote management, Sophos Central offers a robust alternative to WAN admin access. Alternatively, Zero Trust Network Access (ZTNA) can be utilized for remote management. ZTNA provides a more secure approach by ensuring that only authenticated and authorized users can access network resources.
- **Local Services Access Control**: Check your local services access control under *Administration* > *Device Access* and ensure no items are checked for the WAN Zone unless absolutely necessary. Additionally, ensure admin access from your internal LAN is either disabled or limited to specific trusted LAN IPs. Restricting access to trusted IPs adds an extra layer of security by ensuring that only authorized devices can manage the firewall.
- **Remote Users**: Consider ZTNA, which is more secure than VPN. If VPN is used, utilize the new hardened containerized VPN Portal, enabling it only when configurations change and users need updates—otherwise, keep it disabled. Disable User Portal access on the WAN and provide access via VPN only. Use multi-factor authentication on all portals to prevent unauthorized access.

3. Use Strong Passwords, Multi-Factor Authentication, and Role-Based Access

Strong authentication mechanisms are crucial for protecting your firewall:

- **Enforce MFA**: Enable Multi-Factor Authentication (MFA) or One-Time Password (OTP) for all admin and user accounts. This protects your firewall from unauthorized access through stolen credentials or brute force attacks.

- **Strong Passwords**: Enforce the use of strong, unique passwords. Regularly update and audit passwords to ensure compliance with your organization's security policies. Strong passwords should include a mix of letters, numbers, and special characters.
- **Sign-In Security**: Set your sign-in security settings to block repeated unsuccessful attempts and enforce CAPTCHA. This helps to prevent automated attacks and brute force attempts.
- **Role-Based Access Control**: Implement role-based access controls to limit exposure and provide users only the access they need. This minimizes the risk of internal threats by ensuring that users only have access to the resources they require for their job functions.

4. Minimize Access to Internal Systems

Minimizing access to internal systems reduces potential risk:

- **NAT Rules**: Any device exposed to the WAN via a NAT rule is a potential risk. Ideally, no device should be exposed to the internet via NAT or inbound connections, including IoT devices. Ensure that only essential devices and services are exposed.
- **Regular Audits**: Regularly audit and review all your NAT and Firewall Rules to ensure there is no WAN to LAN or remote access enabled. Conduct regular tests to identify and address risky configuration drift. Regular audits help to identify any misconfigurations that could be exploited by attackers.
- **Remote Administration**: Use ZTNA or VPN for remote administration. Avoid exposing systems like Remote Desktop directly to the Internet. Use secure remote access methods that provide strong authentication and encryption.
- **IoT Devices**: For IoT devices, ensure they do not require direct access via NAT and shut down any that do not offer a cloud proxy service. IoT devices can be particularly vulnerable to attacks, so limiting their exposure is crucial.

5. Enable Appropriate Protection

Implementing appropriate protection measures is vital for network security:

- **Intrusion Prevention**: Apply Intrusion Prevention System (IPS) inspection to incoming untrusted traffic and avoid broad firewall rules that allow ANY to ANY connections. IPS helps to detect and block malicious traffic before it can reach your network.
- **DoS/DDoS Protection**: Protect your network from DoS and DDoS attacks by setting and enabling protection under *Intrusion Prevention > DoS & spoof protection*. Enable spoof prevention and apply flags for all DoS attack types. This ensures that your network can withstand and mitigate denial-of-service attacks.

- **Geolocation Blocking**: Block traffic from regions you don't do business with by setting up a firewall rule to block traffic originating from unwanted countries or regions. Geolocation blocking helps to reduce the risk of attacks from high-risk areas.
- **Threat Feeds**: Enable Sophos X-Ops threat feeds to log and drop under Active Threat Protection. Threat feeds provide real-time updates on emerging threats, allowing your firewall to block known malicious traffic.
- **Network Detection and Response**: Use Network Detection and Response (NDR) to monitor traffic to and from the firewall as well as traffic flowing through the firewall for possible attacks. NDR provides visibility into network activity, helping to detect and respond to threats.

6. Enable Alerts and Notifications

Setting up alerts and notifications ensures timely responses to security events:

- **System-Generated Alerts**: Configure Sophos Firewall to alert administrators of system-generated events. Regularly review the list of events to ensure all critical system and security events are monitored.
- **Email and SNMP Notifications**: Notifications can be sent via email and/or to SNMPv3 traps. To configure notifications, navigate to *Configure* > *System Services* and select the Notifications list tab. This ensures that administrators are promptly alerted to any potential issues.
- **Log Management**: Ensure your firewalls send logs to Sophos Central and/or your SIEM of choice for comprehensive monitoring and analysis. Proper log management provides valuable insights into network activity and security events.

7. Segregate Networks and Apply IPS Policies

Separate internet-facing services, such as web servers or remote access servers, into a different network segment and zone from your main LAN. Use a DMZ zone for these services and configure firewall rules to block connections from the DMZ to the LAN. This segmentation prevents malware or hackers from spreading laterally through your networks if an initial attack is successful.

8. Lock Down Remote Access

Restrict access to internal resources via a VPN connection and avoid using port forwarding. If port forwarding is necessary, apply an IPS policy to the rule handling the traffic. This ensures remote access is secure and controlled.

Aishan Technologies

Conclusion

In today's digital age, cyber threats are more sophisticated and frequent. Without robust firewall security, organizations face risks like data breaches, malware infections, and operational disruptions, leading to financial losses and reputational damage.

To protect against these threats, adopting stringent security practices is crucial. This includes regularly updating firewall firmware, limiting device service access, using strong passwords and multi-factor authentication, minimizing access to internal systems, and enabling appropriate protections like IPS and DoS/DDoS protection. Additionally, setting up alerts and notifications, segregating networks, and locking down remote access through VPNs are vital steps.

Aishan Technologies is committed to helping organizations strengthen their network defenses with tailored cybersecurity solutions and continuous support.

By following these best practices, you can significantly enhance your security posture and protect your network infrastructure from evolving cyber threats. For further assistance, please contact Aishan Technologies.

Aishan Technologies

Contact us:

Sophos Gold Partner

Aishan Technologies India Pvt Ltd
No. 13-14, SV Complex, Kothnur Main Road,
Navodaya Nagar, JP Nagar 7th Phase
Bangalore 560078

K. Bharani Nath "Karthik"
M: +91 998 000 2657 | E: karthik@aishan.in