secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Firewall Configuration Security Review

Firewalls are an essential component of network security as they monitor incoming and outgoing network data, either permitting or blocking based on security rules.

Upon initial installation these configurations are often locked down, but then over time as network and business requirements evolve, changes are made which reduce the protection the firewall once offered. A Firewall Configuration Security Review will highlight these areas of weakness, enabling an organisation to reconfigure their firewall rules for better security.

Who Is It For?

Firewalls are designed to be the first line of defence against cyber attacks, making them a fundamental security system that all organisations should be using and reviewing on a regular basis.

Firewall Security Reviews are also required for standards such as Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR), and ISO 27001. Therefore, any organisations needing to comply to these standards should consider this review.

How Can We Help?

It is essential that the configuration and ruleset of your firewall, meets the business and compliance requirements of your organisation. However, its common for firewall settings to be changed and forgotten about over time, or misconfigured leaving your networks open to attackers.

Our Firewall Configuration Security Reviews can provide system administrators with a comprehensive overview of the configuration of your firewall or similar security device, highlighting areas of weakness. This will allow your organisation to understand and remediate any firewall security issues, to ensure that it's as locked down as possible.

What We Test

Our consultants will review your firewall configuration and rulesets, identifying, verifying and prioritising weaknesses based around:

- **Known Vulnerabilities** Missing security updates is a common weakness that can lead to devices being compromised.
- **Authentication Authentication systems** often have weaknesses such as username enumeration, lack of brute force protection, or even just common and weak passwords.
- **Access Control Systems** Where access is granted to hosts, services, or ports, our consultants will review the access to determine if it introduced unexpected weaknesses in the protection or if the allowed access is overly permissive.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

Secarma's Firewall Assessment enables a transparent understanding of the way in which your firewall security-related configurations have been defined, to compliment a defence-in-depth strategy.

Here is a more in-depth explanation of how we assess your firewall configurations.

AUTHENTICATION

Accounts on the device may provide a means to access or administer configurational settings. Often these accounts are configured during initial installation and then neglected, which can lead to a compromise when combined with weak or default credentials

NETWORK MANAGEMENT

Firewalls often have protocols such as SNMP enabled to allow for system monitoring, however these protocols are often insecurely configured which can allow a threat actor to gather information about target systems.

ADVANCED PROTECTION

Many modern security devices have advanced protection options such as Web Filters and Anti-malware solutions. We can review the configuration of these protections to ensure they are enabled and offering the expected protections.

PATCHING & UPDATE STATUS

Just like user workstations, firewall vendor patches and updates are regularly released to ensure that known vulnerabilities are remediated. The device will be reviewed to ensure that these are installed in a timely manner.

RULESET

A major part of a Firewall Configuration Security Review is the firewall ruleset, or access control lists. The access control lists typically control access through approved target/source IP addresses, services, or ports. We review these rulesets to ensure that the rulesets are not overly permissive.