

# Is your front door secure? A Logicalis Firewall Assessment provides you with peace of mind.

**When was the last time you reviewed your perimeter security? Is your firewall configuration up-to-date and aligned with your security policy? Does your firewall allow secure and policy-based authentication of remote devices?**

A Logicalis Firewall Assessment provides documentation to demonstrate you have been undertaking due diligence in reviewing security and policy controls.



Ensuring regulatory compliance requires most organisations to not just maintain a firewall, but to develop a configuration testing methodology. Beyond compliance requirements, a regular firewall audit or assessment increases the likelihood of identifying weaknesses in your network security posture, improving firewall performance and simplifying management.

Research shows that up to 30% of a firewall's policies aren't needed – and excessive configuration complexity can impact performance. Complexity will also negatively impact compliance and security.

Providing remote connectivity to mobile users or new types of devices (such as iPads or smart phones) may require updates to your security policy and changes to firewall configuration (or a new firewall). A Logicalis Firewall Assessment ensures that you gain the benefits of enabling remote connectivity, without introducing new vulnerabilities.

“More than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.” — Gartner



A Logicalis Firewall Assessment reviews your security policy and firewall infrastructure, including configuration. It provides you with a **Security Assessment Document** that outlines recommended changes or updates to security policy, aligned with industry and vendor best practices.

**What can we do for your organisation**

Contact Logicalis to learn how we can help.

Visit [www.au.logicalis.com](http://www.au.logicalis.com)

Call 1800 453 454

- **Workshop with network and security administrators** to determine current practices and firewall functionality. (This also determines the desired security levels within organisation.)
- **Analysis of current network documentation** to determine the placing of the existing firewall and interfaces. This helps determine the optimal location under the new security architecture and identify where any potential vulnerabilities may exist).
- **Detailed device configuration analysis** will be performed against the current security appliance. An audit would be conducted on the access control lists and their current placings within the configuration. Unused access control lists will be assessed to determine whether the new device/configuration needs to have them included.
- **Current remote access deployments will be assessed** and recommendations given in the assessment report.
- **Local authentication, authorisation and accounting policies are audited** against industry best practices to ensure any administration changes to the configuration during normal operations are properly recorded.