



PERIMETER FIREWALLS - POLICY DOCUMENT

Document Id	Firewall Policy
Date	8th June 2017

Version Control Log

Version	Date	Change
1.0	08/06/2017	Initial Draft
2.0	04/08/2022	Updated
2.1	16/10/2024	<p>Policy reviewed by IT contractor: The policies are directly correlated with IASME who are government institute for IT security, they utilize a framework called NIST (National Institute of Standards and Technology) which ensures best practices.</p> <p>This all revolves around your cyber essentials certification (found here: BM Registry 647cf813-f457-453c-8732-61c3708521b6 (blockmarktech.com)). All 3 policies are up to standard.</p>
2.2	08/01/2026	<p>The internet and Email Policy, and Password policy are relevant and accurate. They do not need to be changed or amended.</p> <p>However, whilst the firewall Policy is accurate. The physical firewall equipment onsite needs to be replaced to meet said compliance.</p>

Document Approval

Name	Date
Policy & Resources Committee	07.09.2022
Policy & Resources Committee	12.02.24
Policy & Resources Committee	11.02.26

Introduction and Scope

Newton Abbot Town Council (NATC) maintain perimeter firewalls at each internet connected location to establish a secure environment for the network and computer resources at each location.

These firewalls filter internet traffic to mitigate the risks and potential losses associated with security threats to the network and information systems.

Firewalls are defined as security systems that control and restrict network connectivity and network services.

The perimeter firewalls are an essential component of the Newton Abbot Town Council's security architecture.

The scope of this document covers devices that filter, control and protect at the network layer. Filtering at the application layer is not within the scope of this document.

Our outsourced IT Service Provider (ITSP) is Alchemy Systems (Western) Ltd.

Purpose

The purpose of this policy is to define standards for provisioning security devices owned and/or operated by NATC. These standards are designed to minimize the potential exposure of NATC to the loss of sensitive confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of NATC resources.

This policy establishes procedures for NATC's perimeter firewall administration, determines the technology standard used by the firewall hardware and software, assigns firewall administration responsibilities and defines the filters applied to the networks.

Responsibilities

The outsourced ITSP is responsible for implementing and maintaining the company's perimeter firewalls and is also responsible for activities relating to this policy.

While responsibility for information systems security on a day-to-day basis is everyone's responsibility specific guidance and direction for information systems security is the responsibility of the ITSP. The ITSP will manage the configuration and patching of the NATC firewall.

Policy for Perimeter Firewalls

The perimeter firewall permits the following outbound and inbound Internet traffic:

- Outbound Policy - All Internet traffic permitted to hosts and services outside of NATC's networks except those specifically identified and blocked as malicious sites.
- Inbound Policy - Default deny policy but allow unsolicited inbound traffic that supports the needs of the business and where there has been an analysis of risk and that risk is deemed acceptable and a written business justification made.

Open ports must be documented in the Firewall Ports Open List document stored at the ITSP.

Reason for filtering ports or applications:

- Protecting the network - Certain ports are filtered to protect the networks users.
- Protecting the outbound bandwidth - Traffic may be restricted using polices or rules to ensure that an acceptable service level is maintained across the business for all users.

Firewall Standards

Newton Abbot Town Council is committed to operating fully supported, maintained and resilient firewalls.

Operational Procedures (Perimeter security)

NATC staff may request that access be granted from the Internet to services inside NATC for a new or existing application or service. These requests must be made in writing using the "Firewall Change Request Form". The request should be sent to support@alchemysys.co.uk. It must include a justification to support the request.

The ITSP will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the requestor and alternative solutions will be explored.

It should be expected to require standard services to run on standard TCP/UDP ports.

Certain mission-critical functions require outside entities to have secure, limited access to NATC information systems achieved by way of the Internet. Such access must be requested and approved in the same way.

Change Management Procedures

Configuration changes must follow the appropriate change management procedure. All updates to existing rules are considered 'business as usual' and therefore can be scheduled outside the change management process. Addition of new rules or large configuration changes would be considered for a configuration change request.

Periodic Review of Firewall Settings

New rule-sets for services are reviewed by the ITSP before firewall changes are implemented. Alternatively, when an application is phased out or upgraded, the firewall rules set is changed. This approach adds some rigor and discipline to the firewall policy implementation, minimising the presence of old and potentially insecure rules that are no longer needed.

Firewall installations and rule-sets should be audited on a quarterly basis. Firewall firmware should be upgraded at least every quarter to the latest release.

The *Firewall Ports Open List* should be maintained to keep an accurate list of all ports open and this should be updated during any audit. External scanning should be completed to ensure that only the ports intended are open.

This Firewall policy will be reviewed annually. It is next due to be reviewed in June 2023.