
# Firewall Management Policy

(Physical appliances only)

| Document Control | |
|---|---|
| Title: | Firewall Management Policy |
| Issued by: | Information Security |
| Date: | 7th August 2019 |
| Author | Michael Parker |
| Version: | 2.0 |
| Status: | Released |
| Protective Marking: | Official |

Revision History

| REVISION | DATE | REVISION STATUS |
|---|---|---|
| 1.0 | 11/04/2017 | Released |
| 2.0 | 07/08/2019 | Released |

Document Review

| REVIEWER | POSITION | DATE |
|---|---|---|
| Michael Parker | Senior Information Security Officer | 08/05/2019 |
| Graham Dunnings | Security Consultant | 08/05/2019 |
| Morgon Evans | Cyber Security Manager | 07/08/2019 |

# Introduction

If you are going to deploy, (re)configure, or decommission any Warwickshire County Council (WCC) managed firewall (this includes, but is not limited to, any Core Network Firewall, Boundary or Perimeter Firewall, or remote site Firewalls) then this policy is the one for you.

Throughout this policy the words MUST, MUST NOT, SHOULD, SHOULD NOT, ONLY are used. Their respective definitions for the purpose of this policy are:

- **MUST** - This word, or the terms "REQUIRED" or "SHALL", will mean that the definition is an absolute requirement of the policy.
- **MUST NOT** - This phrase, or the phrase "SHALL NOT", will mean that the definition is an absolute prohibition of the policy.
- **SHOULD** - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully risk assessed before choosing a different course.
- **SHOULD NOT** - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **ONLY** - This word will mean that this option is the only permitted choice allowed.

# Purpose

The purpose of the policy is to set out how Firewalls managed by WCC are to be commissioned, configured, maintained and decommissioned.

# Scope

This policy shall be enforced for all staff, contractors, agents or any 3rd party working for or on behalf of WCC for the purposes of work on or with any Firewall implemented or managed by

WCC. This includes, but is not limited to, any Core Network Firewall, Boundary or Perimeter Firewall, or remote site Firewalls.

## Out of Scope

Client or Host Based Firewalls (I.E. Microsoft Firewall)/IP Tables etc. Virtual Firewalls including cloud environments.

## What to do if I am unable to meet the requirements within this policy (Non-compliance and Exceptions)?

When it is impossible to comply with this policy or a business reason dictates; a risk assessment MUST be made by Cyber Security via a logged service desk call detailing the business reason for the exception. The team will review this, and the final decision rests with the Cyber Security Manager. If an exception to the policy is agreed then it MUST be recorded in the Information Security Policy Exceptions Register (ISPER).

Should this policy be breached and the instance is not recorded on the Information Security Policy Exceptions Register (ISPER) or no attempt has been made to do so, WCC may take disciplinary action against the individual(s) which may include Summary Dismissal for Gross Misconduct pursuant to the employment contract, it may also include escalation to law enforcement authorities where a breach of any relevant law has or is reasonably believed to have taken place.

## Who do I contact if I am unsure about anything within this policy?

All enquiries MUST be made to Cyber Security via a logged service desk call.

## Definitions

**Firewall** - a device that separates two networks and controls the network traffic which flows between them.

**Intrusion Prevention System (IPS)** - a method that inspects network traffic that is processed by a Firewall and looks for patterns which can provide a risk to the network infrastructure and seeks to either actively block or reject this traffic from being processed. You may hear the term Intrusion Detection System (IDS) used and this is roughly a passive version of an IPS, which does not actively block or reject this traffic and/or network devices based on any results.

**VPN** - Virtual Private Network - a method of connecting two networks together via an encrypted tunnel over an untrusted or public network.

# Policy - General

**Procurement and Provisioning**

1. Any WCC Firewall MUST be fit for purpose and scalable for its intended environment, its selection MUST adhere to any HMG guidance for the processing of data classified as OFFICIAL.

2. If WCC have a preferred supplier of Firewalls, these must be considered above anything else to ensure the central management of the Firewall estate.

3. **New sites** using ADSL/VDSL connections MUST have the suppliers “Broadband Router” replaced so the remote site can be linked to WCCs network via a VPN. This ensures that WCC can both manage the devices on the remote network and can control what access that remote site has. An assessment MUST be made to select suitable controls and MUST be approved by the Cyber Security Manager.

4. **Existing sites** using ADSL/VSDL MUST have their gateway or “Broadband Router” replaced as soon as possible to ensure all remote sites are managed and any firewall access policy is consistent across WCC.

5. Any Firewall acting as a gateway to the HMG ‘PSN’ Network, MUST be a separate physical firewall; it MUST NOT be a virtualised firewall (i.e. a VM) in a shared chassis or network segment in a switched firewall.

**Configuration and Change Management**

6. Any firewall, either remote or local, MUST have any defaults changed. This includes any passwords and to ensure that the rules are configured on a Default Drop and only permit the access that has a business need. The device once initially configured for production MUST then be placed under change control.

7. All administrative user interfaces MUST be disabled on any public facing interfaces.

8. All logging SHOULD be enabled if available and these logs SHOULD be actively monitored for suspicious behaviour. It SHOULD post these logs to an off device central log management system. It is acceptable to configure the firewall to ignore certain types of log entries as a firewall log file is likely to contain a lot of data. E.g. It may be acceptable to log outgoing traffic but ignore incoming connection attempts. There may be services/ports that you wish to include for a more verbose logging. If in any doubt or you would like further guidance please contact Cyber Security Team.