# Firewall Rules Guidelines

## | Document Information |

Category: Architecture Guidelines |  
Created: 2022-03-22 |  
Domain: Security |  
Author: pete.dingwall@education.gov.uk |  
References: PRI-SEC004 - Firewall Guidelines |

## Baseline guidelines for firewall rulesets and access

The following guidelines are provided to guide Department operational teams when creating and maintaining firewall policies, and managing requests for access from the Department’s delivery and operational teams

**Exceptions** to the guidelines will be reviewed with the security and architecture governance teams and approved or declined as relevant, with all decisions tracked with rationale for future reference.

**Updates or modifications** to the principles can be requested via the owning architect, and will be reviewed against the roadmap and strategy and within the Architecture profession.

**Escalations** will be dealt with within the immediate leadership within the relevant architecture domain (up to DD level) and to the SLT by exception.

## Introduction

The guidelines are provided for baseline guidance for the definition of firewall policies and management of firewalls, and to provide an understanding of the common and non-standard ports and protocols used within the Department,

## Manage admin access appropriately

#### How?

*Review PRI-SEC001 (Authentication principles) and follow guidelines to secure administrative access*

#### Why?

* Following least privilege at all times ensures that any changes are made consciously and appropriately
* Using a well-defined role-based access control (RBAC) method ensures that permissions required to manage the platform are appropriate
* Using a Just-In-Time access model, complemented with the least-privilege model, ensures that access is only provided when required for the specific task
* Separation of Duties must be followed to ensure that teams managing multiple environments only have access to the specific environment and service (Dev/UAT/Prod etc)
* Restricting access from DfE devices (not from BYO or 3rd party) ensures that the access is protected and secured appropriately

## General guidelines for firewall rules

### Block inappropriate traffic

#### Why

* block rfc 6761 1918 4913 for inbound or Internet access
* drop from server vlans not dmz
* Outbound blocked from servers in DMZ other than for their service
* Block broadcast
* Use deny-all

### Enable access consciously and limit to least-access

* Open up consciously
* Limit access to only what's required

### Restrict access to services which could enable direct Internet access

* Web access from all devices is via a proxy, no direct access to services
* DNS access from clients not permitted, resolution only via our managed DNS to stop direct access

### Use automation if available

* Use automated feeds for cloud services to manage dynamic IP ranges (MS RSS for Azure etc)
* Investigate PA ability to take live feeds
* Threat feeds

### Services are responsible and accountable for their access

* Services must document and validate any outbound or inbound requirements
* Services must consider their attack surface and only open what’s required
* Recertification of inbound and external access every X months
* simple as someone ticking "still required" but audited and risk owned by person ticking the box
* Known IP ranges is a brittle control and should be used as part of a defence-in-depth strategy

### Run services on standard ports

* No running of standard services on non-standard ports (obfuscating RDP access)

### Access is only granted to valid endpoints

* Remote endpoints using registered and valid domains
  + no URL shorteners (ow.ly, bit.ly etc)
  + no dynamic DNS domains
  + no consumer-level services
  + no consumer hosting platforms (GoDaddy, SquareSpace, Wordpress etc)

## Logging

* admin access logs into Splunk
* Firewall logs to Panorama, with critical alerts and important messages into Splunk

## Outbound access

### Defaults

The following services and protocols are allowed outbound by default for public-facing services within DMZs:

|  |  |
| --- | --- |
| Service | Protocol & Port |
| http | TCP 80 |
| https | TCP 443 |

### On-request

The following services and protocols are allowed outbound with conscious approval and demonstrated business need:

|  |  |  |
| --- | --- | --- |
| Service | Protocol & Port | Caveats |
| DNS | TCP/UDP 53 | Internal DNS servers requiring external lookup |
| SMTP | TCP 587 | Internal operational mail servers requiring outbould relay |
| IMAPS | TCP 993 | Internal mail servers requiring inbound mail |
| NTP | TCP 123 | Approved NTP servers within the Stratum hierarchy |
| SSH | TCP 22 | Agreed endpoints and services |
| MSSQL | TCP 1433 | Agreed endpoints and services |

## Inbound access

### Defaults

The following services and protocols are allowed outbound by default for public-facing services within DMZs:

|  |  |
| --- | --- |
| Service | Protocol & Port |
| http | TCP 80 |
| https | TCP 443 |

### On-request

The following services and protocols are allowed outbound with conscious approval and demonstrated business need:

|  |  |  |
| --- | --- | --- |
| Service | Protocol & Port | Caveats |
| VPN | UDP 1194 | Permitted for the Department’s main remote access solution |
| SMTP | TCP 587 | This may not be required |
| SFTP | TCP 22 | (for specific encpoints which need to securely and programatically exchange data) |
| FTPS | TCP 900 | as above |
| DNS? | TCP 53 | (depending on how our DNS is currently structured, if we host zones etc) |

### Not Permitted

Any protocols and services which are not listed in the Inbound and Outbound Access sections are not permitted. Services will be updated and iterated for other approved services following approved demand from delivery and operations areas.

Common *not permitted* services are outlined below, with rationale and guidance for services which provide a suitable alternative.

|  |  |  |
| --- | --- | --- |
| Not-permitted service | Rationale | Equivalent service |
| FTP | Unsecure service | SSH |
| Telnet | Unesecure, legacy service | SSH |
| Telnets | Legacy service | SSH |
| RDP | RDP sevices are a regularly exploited and a security risk | (jump box strategy) |
| File services protocols SMB, NFS etc | Unsecure, regularly exploited service | SFTP |
| Legacy auth traffic (Kerberos, NTLM) | Not designed for WAN/Internet use | OIDC, SAML 2.0 |
| LDAP/LDAPS | Potential for exposure if poorly implementated | No business need |
| Remote access and tunelling protocols | Could be used to circumvent standard protective controls | No Business Need |
| Legacy name lookup services (WINS) | Not designed for WAN/Internet use | DNS |
| IP6to4 protocols? | Could be used to circumvent standard protective controls | No Business Need |