**Firewall Principles**

**Allowed outbound**

* https
* HTTP

**Allowed outbound with conscious approval and business need**

* DNS (restrict to known)
* SMTP (restrict to known)
* IMAP (restrict to known)
* NTP (restrict to known)
* ssh (restrict to specific groups, investigate more)
* MSSQL (restrict to known endpoints)
* M365 services (Teams etc)

**Allowed inbound**

* https
* http

**Allowed inbound with conscious approval and business need**

* VPN (for the main RA solution)
* SMTP (may not be required, as we use Exchange Online)
* SFTP (for specific encpoints which need to securely and programatically exchange data)
* FTPS (990) - as above
* DNS? (depending on how our DNS is currently structured, if we host zones etc)

**Do not allow**

If not listed in this guideline it's blocked. The items below will be called out specifically to confirm what to do instead

* FTP
* Telnet
* Telnets
* RDP (jump box strategy)
* file services protocols SMB, NFS etc
* Legacy auth traffic (Kerberos, NTLM)
* LDAP/LDAPS
* Remote access and tunelling protocols (ppp, pppoe, LT2P, IPSEC VPN)
* legacy name lookup services (WINS)
* IP6to4 protocols? (could be used to mask access, maybe I’m being paranoid!)

**Admin access**

* least privilege at all times
* defined RBAC
* JiT access
* teams managing multiple environments still need separate groups
* SoD etc (refer back to the principles)
* Access only permitted from DfE devices, not from BYO (DfE 'device' could be a virtual endpoint, jump server)

**General guidelines for firewall rules**

* block rfc 6761 4913 for inbound access
* drop from server vlans not dmz
* Outbound blocked from servers in DMZ other than for their service
* Block broadcast
* Use deny-all
* Open up consciously
* Limit access to only what's required
* Use automated feeds for cloud services to manage dynamic IP ranges (MS RSS for Azure etc)
* Known IP ranges is a brittle control and should be used as part of a defence-in-depth strategy
* Services must document and validate any outbound or inbound requirements
* Services must consider their attack surface and only open what's required
* No running of standard services on non-standard ports (obfuscating RDP access)
* Investigate PA ability to take live feeds
* 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
* Remote endpoints using registered and valid domains
  + no URL shorteners
  + no dynamic DNS
  + no consumer services
  + no consumer hosting platforms (GoDaddy, SquareSpace, Wordpress etc)
  + 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

**Logging**

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

**Web filtering**

* Everyone gets Business and News
* Social for those who require it (pending a review of allowed services)
* Developer for those who require it (pending a review of allowed services)
* sites enabled with clear business need only
  + be clear that all access is monitored, including SSL (if privacy is important, don't use your work PC
* Should apply to all, including BYO (if they want to access DfE's services in future, we'll block traffic to only allow from proxy endpoints)

Process to manage will be

1. ServiceNow request to log
2. If it's a specific group approval should be straightforward if their job matches the request
3. If it's a business need for specific site(s) will need to be reviewed by ???

Any shift-left should be with a well-designed service and clear guidelines, can't just transfer a poor process over with lots of steps/work