iQuda firewall security infrastructure policy

The iQuda IT Infrastructure operates perimeter Firewalls/Gateways between their Internet and the iQuda LAN infrastructure. This configuration also applies between segmented areas of LAN to establish, and enforce security of iQuda resources, and assets, and thus, this Firewall Security Infrastructure are key components of the logical security defence.

Purpose

This policy defines the standards for provisioning security devices owned and/or operated by iQuda users. These standards are designed to minimise the potential exposure to iQuda systems, and assets, as well as providing protection against loss of business sensitive, confidential information assets, or causing any exposure to associate, and/or business partner from unauthorised access.

Procedures

This policy establishes procedures for Security Infrastructure Firewall Administration, determines the technology standard to be used by Firewall hardware and software, and assigns the approach to Firewall Administration responsibilities, and the high-level filters to be applied to iQuda networks.

Scope

This Firewall Policy refers to the Firewall Security Infrastructure, to govern and protect iQuda resources and assets, be they *physical*, *logical* or *information* assets. All Firewalls and other devices serving a Firewall capability within Security infrastructure fall under the scope of this policy.

Firewall Function

The Firewalls at minimum functionality perform the following security services to protect iQuda resources and assets:

- Access control between the *trusted* internal network and any *untrusted* external networks
- Block unwanted traffic as determined by the applied Firewall Rule-Set
- Protect internal business critical assets and systems from the internet exposure
- Obfuscate information, such as system names, network topologies, and internal User-IDs, from internet visibility
- Log traffic to and from the internal network
- Provide robust authentication mechanisms as required
- Provide support to remote access solution when necessary (e.g. Third Party)

Administration Responsibilities

The iQuda System Administrator (James Watson, Technical Director) is responsible for implementing and maintaining Firewalls, as well as enforcing and managing Firewall Rule-Sets. Logon access to the Firewalls

will be restricted to this role only (or any other authorised, delegated Administrator). All other users will be *denied* access to Firewall Administration facilities and access by default.

If you need to discuss any aspect of firewall security with someone, please address your questions to James Watson.

Firewall Security Infrastructure

iQuda Firewalls will generally block all inbound and outbound traffic that have not been *expressly* permitted by the Firewall Policy. This rule is by default known as, "*deny-by-default*", or the "*stealth rule*".

Firewall Rules-Sets (Policies) will only permit the necessary protocols through the Firewall Security Infrastructure that are required to support the business. For example commonly used IP protocols are:

- ICMP (Internet Control Message Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Control)

The following are the Baseline Standard for managing the iQuda Firewall Security Infrastructure:

- Other IP protocols such as IPSec components Encapsulating Security Payloads (ESP), Authentication Header (AH), and routing protocols may also need to pass through Firewalls. However, again this will only be expressly permitted where a business requirement has been identified.

- All necessary protocols will be restricted whenever possible to the specific hosts and networks, and only enabled on justified iQuda business requirements. All unnecessary protocols are *denied* by default.

- It is a mandatory control that any electronic equipment that processes or communicates with, or interfaces to any external or public network will pass through Firewall Security Infrastructure.

- The Firewall Security Infrastructure must record all *inbound* and *outbound* traffic and save to logs, which must be stored in a secure location. Recommended period for log retention is one year (rolling). Any extension to this retention period must be approved in writing by the iQuda Managing Director (Anthony Jones).

- Any Remote Administration communicating to the iQuda Firewall Security Infrastructure must be performed over secure channels. E.g. an encrypted network connection using SSH or Console Access.

- Only the authorised System Administrator(s), Anthony Jones, James Watson or Stephen Macintosh are allowed to log on to the Firewall Security Infrastructure.

- All Firewall Rule-Sets must be recorded and reviewed annually for any changes.

- The default settings for the Firewalls *deny* access to any (all) untrusted networks by default. However, if access is required to any networks annotated as *untrusted*, they must be justified to

have a business requirement, and then only allowed after they have been approved by Anthony Jones prior to facilitating access.

- All Firewalling Security Infrastructures must be kept up to date with latest patches, and hot fixes.

- All Firewall Security Infrastructure Servers must be hardened to prevent any security breaches caused by vulnerability or other exposure or cause.

- Any changes to Security Infrastructure must be authorised by Anthony Jones. The QRF iQuda Change Request Form must be used to request changes, and changes must be preapproved before being made.

- All applied, or modified Rule-Sets made to the iQuda Firewall Security Infrastructure must be reviewed by a second technically competent person prior to them being promoted to the production environment of the Firewall Security Infrastructure.

- All Rule-Sets applied to the iQuda Firewall Security Infrastructure will be backed up and secured in a location under the control of the Systems Administrator(s). This equally applies to any Backup Rule-Sets.