FIREWALL

POLICY DOCUMENT

Document Id	Firewall Policy
Sponsor	Laura Gibbs
Author	Nigel Rata
Date	May 2014

Version Control Log

Version	Date	Change
1.0	15/05/12	Initial draft for review
1.1	15/05/14	Update

Document Approval

Name	Approval Signature	Approval Date
ITUAG	Approved	27.5.14

Introduction and Scope

The Royal Holloway University of London (RHUL) Information Technology Services manages a perimeter firewall between its' Internet connection with JANET and the RHUL campus network to establish a secure environment for the campus' network and computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the campus network and information systems. In addition the firewall secures a number of other 'zones' controlling traffic between clients and servers and other parts of the RHUL data network.

The perimeter firewall is a key component of the institution's Network Security Architecture.

Purpose

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

This policy establishes procedures for RHUL'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 campus networks.

Responsibilities

The Network's team within IT Services (part of IT Service Delivery) is responsible for implementing and maintaining the institution'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 Information Systems. The Networks Team will manage the configuration of the University's firewalls.

Policy for Perimeter Firewalls

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

• Outbound - All Internet traffic to hosts and services outside of RHUL's networks except those specifically identified and blocked as malicious sites.

• Inbound - Allow Internet traffic that supports the mission of the institution and is in accordance with defined system, application and service policies.

A description of the other security zones implemented by the RHUL perimeter firewall is outlined in appendix A.

The configuration of the security zones and their use is the responsibility of the IT Infrastructure Manager.

Reason for filtering ports or applicatons:

• Protecting RHUL Internet Users - Certain ports are filtered to protect RHUL networks and users.

• Protecting our outbound bandwidth - If RHUL Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other RHUL systems.

• Protecting the rest of the Internet - Some filters prevent personnel who are associated with the University from both knowingly or unknowingly attacking other computers on the Internet. In addition to being in RHUL's interests for protecting our bandwidth, it is the institutions' responsibility to prevent abuse of its network.

Firewall Standards

RHUL is committed to operate fully supported and maintained resilient enterprise class firewalls.

Access to read or write firewall configurations for both internal or perimeter devices are required to be by unique identity which can be logged.

Policy for Internal Firewalls

Internal firewalls are in place to establish secure communications between the different segments of the University's network where different levels of security and/or protection are warranted. At RHUL centrally managed internal firewalls exist and are the responsibility of IT services to maintain. There are some academic department based firewalls and the responsibility for their administration lies with the academic department. Installation of an internal firewall needs to be approved by the IT Infrastructure Manager. Administrators of internal firewalls should expect IT Services to influence specification, network connectivity, network design and rule sets of any existing or new installation.

Operational Procedures (Perimeter security)

RHUL staff may request that access be granted from the Internet to services inside RHUL for a new or existing application or service. These requests must be approved, authorized and submitted to the Networks Team by appropriate individuals within the University and must include a justification to support the request. The request should be made to itservicedesk@rhul.ac.uk.

The Networks Team 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 limitations and the availability of required resources to implement the request. 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.

Users should expect IT Services to require standard services to run on standard TCP/UDP ports.

Certain mission-critical functions require outside vendors and other entities to have secure, limited access to campus information systems achieved by way of the Internet. Such access must to be approved and then coordinated using the 3rd Party access policy.

If the original requestor considers the solution to be not properly suited to meet their needs, the request can be reviewed by the IT Infrastructure Manager.

Requests that are for access to existing service will be processed using the procedure above as the process includes adding details to existing rules. If the request if for access to new services the request will be 1st reviewed by the Network Team and then be passed to the IT Infrastructure manager for approval to generate new rules within the firewall configuration.

Operational Procedures (Internal security)

The main procedures are as above. Additional notes:

- Security zones are added by networks staff with authorisation from the IT Infrastructure Manager.
- Rules and additions to rules that conform with the policy outline in appendix A can be actioned by IT network staff.
- Requests that deviate from the policy must be authorised by the IT Infrastructure Manager.

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 Networks Team 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, minimizing the presence of old and potentially insecure rules that are no longer needed.

Firewall installations and rule-sets should be audited on an annual basis.

This Firewall policy will be reviewed annually.

Appendix A

Untrust – security zone for RHUL internet traffic.

Server – Security zone for backend servers. Inbound access restricted to administrative tasks/systems from internal RHUL networks only.

DMZ – Houses servers with internal and external (to RHUL) access requirements. Most services are proxied via the Enterprise Traffic Managers who's front end interfaces reside within this zone. Inbound access is mostly single ports with standard service combinations, e.g. HTTPS over TCP/443.

Restricted Zone – Security zone for servers with more permissive access requirements, for example databases that require multiple ports open for direct client access or Active Directory domain controllers. Inbound access as per individual server requirements.

VPN – Security zone housing endpoints for remote VPN clients. Restricted outbound access to RHUL networks. No inbound access.

RHUL – Security zone containing the majority of remaining RHUL networks, i.e. academic departments – equivalent of the "trust" zone. Minimal inbound access from external networks, with a permissive outbound access.

Eton College – Security zone for Eton College network traffic.

Enterprise Centre – Part of the RHUL untrust zone - for RHUL Enterprise Centre network traffic