Essex Partnership University
NHS Foundation Trust

EPUT Firewall Policy

POLICY REFERENCE NUMBER	CP77
VERSION NUMBER	V1.0
KEY CHANGES FROM PREVIOUS VERSION	Not Applicable
AUTHOR	[redacted] – Cyber Security Manager
CONSULTATION GROUPS	ICT
IMPLEMENTATION DATE	June 2019
AMENDMENT DATE(S)	Not Applicable
LAST REVIEW DATE	Not Applicable
NEXT REVIEW DATE	June 2022
APPROVAL BY INFORMATION GOVERNANCE & SECURITY SUB-COMMITTEE	28th March 2019
RATIFICATION BY QUALITY COMMITTEE	13th June 2019
COPYRIGHT	

POLICY SUMMARY

This policy provides the list of controls that are required to secure firewall implementations to a NHS Digital approved level of security. This policy provides a list of security controls to protect operational data filtered by firewalls. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

The Trust monitors the implementation of and compliance with this policy in the following ways;

Regular monitoring of firewall configurations by IT Service personnel.

Services	Applicable	Comments
Trustwide		
Essex MH&LD		
CHS		
ICT	✓	

The Director responsible for monitoring and reviewing this policy is Director of Information Technology and Telecommunication

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

EPUT FIREWALL POLICY

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

FIREWALL POLICY

Assurance Statement

This policy provides assurance to the following requirements laid out by NHS Digital to comply with the Cyber Essentials Plus requirements –

Each open connection (i.e. allowed ports and services) on the firewall has been subject to approval by an authorised business representative and documented (including an explanation of business need). Vulnerable services (e.g. Server Message Block (SMB), NetBIOS, Telnet, TFTP, RPC, rlogin, rsh or rexec) have been disabled (blocked) by default and those that are allowed have a business justification. Firewall rules that are no longer required have been removed or disabled. Firewall rules are subject to regular review.

1.0 PURPOSE

1.1 The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to departmental security standards, which are based upon best practice for secure firewall deployments laid out by NHS Digital and the National Cyber Security Centre.

2.0 EXCEPTIONS

2.1 Any exceptions to the application of this policy, or where controls cannot be adhered to, must be presented to IT Services for submission to the Information Governance Steering Sub Committee where appropriate. This must be carried out prior to deployment.

2.2 Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this policy.

2.3 Exceptions to this standard must be maintained on the Trust risk register for accountability, traceability and security governance reporting to senior management.

3.0 AUDIENCE

3.1. This policy is intended for EPUT IT staff and its suppliers, involved in securing firewalls for EPUT systems and provides the security requirements on how to secure them.

4.0 SCOPE

4.1. This policy is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP), including the handling caveat OFFICIAL-SENSITIVE.

4.2. All of the organisation's firewall implementations falling within this category will be subject to the requirements specified within this security standard.

4.3. The requirements will be applied to new and existing installations.

4.4. The security control requirements laid out in this policy are product agnostic and applicable for all firewall systems that are provisioned for Trust use.

5.0 SECURITY CONTROL ASSURANCE

5.1. Controls presented in this policy, or referred to via this policy, may be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness.

6.0 TECHNICAL SECURITY CONTROL REQUIREMENTS

6.1. In this document the term must, in upper case, is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section 2. Exceptions above).

7.0 CHANGE MANAGEMENT

7.1. Firewall changes are a necessary ongoing process that ensures firewall rules are continuously capable of preventing security breaches. A well-defined management plan must include the following:

7.2. A detailed plan of changes and their objectives

7.3. An estimation of risks due to the policy changes, their expected impacts, and a mitigation plan if required.

7.4. A centralised change-management workflow and change-control policy between different network teams and proper change approvals, authorised by a suitably empowered individual that includes an assessment of the rule changes against the live service.

7.5. Proper audit trails of the change including who made the change, when they made it, and the outcome of the change.

8.0 TESTING

8.1. Any planned policy or rule changes must be tested prior to committing to a change to avoid unexpected detriment to the network.

8.2. The following steps must be taken to test Firewall policy and rule changes:

8.3. Trace the path of packet traversal through the network layer and confirm that all devices along the path allow the packet to reach its intended destination.

8.4. Confirm that the firewall is allowing and blocking data according to the established policies and rule sets.

8.5. Perform an analysis to identify which device policies or rules are blocking the packet from reaching its destination.

8.6. Where feasible, the policy or rule changes should be tested in a suitable nonproduction environment before being pushed to the active live environment. Where this is not feasible and the change has to be applied to the active live environment, the change must not be closed down until the policy / rules have been tested and validated to work as expected. Where testing fails, back-out should be made to a previous version of the policy / ruleset.

9.0 RULE MANAGEMENT

9.1. Firewall rule management is a critical activity. Without effective rule management there might be many firewall rules, objects redundancies, duplicate rules, and bloated rules that can negatively affect firewall security, performance and efficiency.

9.2. Redundant or duplicate rules must be removed as they slow firewall performance due to processing more rules in sequence.

9.3. Orphaned or unused rules must be removed as they complicate rule management - Project decommissioning must remove any associated firewall rules.

9.4. Be mindful of shadowed rules as they can leave any other critical rules unimplemented i.e. a broader rule matching a set of criteria is configured above a more specific rule.

9.5. Conflicting rules must be amended as they may create backdoor entry points.

9.6. Be mindful of erroneous or incorrect rules with typographical or specification inaccuracies as they can cause rules to malfunction

9.7. All rules, and changes to rules, must be quality assured by an independent person to remove typos and errors before being implemented.

9.8. All rules and objects should use naming conventions that make the rule base easy to understand. For example, use a consistent format such as host name IP for hosts.

9.9. Where a firewall is shared amongst multiple projects/products, consider including a reference to the service name/code in a firewall change log to help keep track of which rule belongs to who.

9.10. All rule changes must contain a valid change reference so that they can be tracked back to the change record and approver.

9.11. Rules must be prioritised in proper logical order to ensure that the firewall processes them according to the security requirements of the firewall policy. Always place more specific rules first and general rules last.

9.12. Rules that belong together must be grouped.

9.13. You should not use ANY in port number, source or destination address on inbound connections except by authorised exception.

9.14. You must never create an ANY, ANY, ANY or equivalent ALLOW ALL rule on inbound connections, as this may result in allowing every service through the firewall.

9.15. Any rules that can't be assigned to a known product, project or service owner should be monitored for traffic for 30 days. If traffic is not detected the rule should be disabled and left in place for a minimum of 6 calendar months. If after this time a request is not made to re-enable the rule it should be removed and the change logged.

9.16. Any objects that define multiple networks should be reviewed at least annually, to ensure they remain valid.

9.17. Expiry dates must be added to temporary rules and reviewed at least annually for rule clean-up

9.18. Any significant project change should include a review of its associated firewall rules.

9.19. The entire firewall ruleset should be reviewed at least annually to confirm alignment with the standard, remove defunct rules, as an audit function, and to identify any vulnerable rules.

9.20. If the firewall supports notes or in-rule documentation, extensive use should be made of it.

10.0 AUDITS

10.1. Firewall policy audits are necessary to ensure that firewall rules are compliant with organisational security regulations as well as any external compliance regulations that apply.

10.2. A firewall security audit must take place when a new firewall is installed, and annually thereafter.

10.3. A firewall security audit must take place when firewall migration activity is occurring on the network.

10.4. A firewall security audit must take place when there is bulk configuration changes made on firewalls

10.5. If supported, rule-counters should be used to determine how often a rule has been used.

11.0 USER ACCESS & AUTHORISATION

11.1. It is important to institute stringent network-access security and user-permission control to ensure that only authorised administrators have access to change firewall rules.

11.2. Where possible, network configuration management techniques should be adopted to monitor firewall configuration changes in real time and provide alerts if there are unwarranted configuration changes.

11.3. There must be a configuration restore option in place when unexpected or incorrect configuration changes have been made on the firewall and you need to revert back to an earlier state.

11.4. To support this, backups of the firewall configuration must be taken every time a change is made, with at least 10 backups being kept for analysis should the need arise.

11.5. Firewall logs must be monitored to identify any unauthorised break-in attempt on the firewall from both inside and outside the network.

11.6. Users in charge of managing firewalls must do so via individual administrative accounts provisioned for that purpose, managed on a centralised basis, and authenticated using an appropriate protocol, such as RADIUS, TACACS or LDAP.

11.7. No firewall changes beyond initial configuration required to enable a secure authenticated connection should be performed using local accounts.

11.8. Local accounts may exist for use in emergencies only, but these must be appropriately secured and their use audited.

11.9. All firewall management must be conducted from a dedicated management network that maintains separation from other network security domains.

12.0 INGRESS & EGRESS TRAFFIC FILTERING

12.1. Egress traffic filtering is required to help mitigate the threat of data exfiltration.

12.2. Ingress traffic filtering is required to help mitigate the threat of malware, spoofing and denial-of-service attacks.

12.3. This can refer to firewalls separating a higher security domain from a lower one, but can also refer to separation between two equal level domains.

12.4. IP spoofing must be blocked.

12.5. You must only allow ingress connections from approved and risk assessed end points.

12.6. Vulnerable services (e.g. Server Message Block (SMB), NetBIOS, Telnet, TFTP, RPC, rlogin, rsh or rexec) must be disabled.

12.7. Outbound traffic from VLAN workgroups or entire network segments that have no need establishing client connections to internet servers must be dropped.

12.8. Broadcast traffic must be dropped unless an exception is made (please refer to section 4. Exceptions above).

12.9. All unauthorised traffic should be blocked from entering or leaving the firewall boundary.

12.10. Outbound traffic with destinations that are listed on DROP filter lists must be dropped.

12.11. Similarly, inbound traffic from such destinations must also be dropped.

12.12. Only allow client hosts to access authorised services from authorised external servers

12.13. For inter-server communications involving external servers, only allow access to service ports your internal servers must use to operate correctly. Care needs to be taken regarding ports on a Windows server that are not normally permitted through a firewall.

12.14. Block routing protocols at the firewall - firewalls should not perform dynamic routing. Static routes only.

12.15. If DNS is provided internally, or uses a split DNS, use internal resolvers as forwarders for the internal networks

12.16. If an HTTP proxy, or a proxy system that performs web URL or content filtering is deployed, only allow outbound client web connections through the firewall via the proxy/proxies

12.17. If services are authorised that make use of unique ports for remote desktop, subscription, or licensing channels, only allow access to these services from hosts that are authorised to use them

12.18. Firewalls should silently drop packets and never reject them i.e. never send a TCP RST or ICMP destination unreachable and acknowledge the device's existence.

12.19. Implement rate limiting on ingress traffic to mitigate against Denial of Service attacks.

13.0 UPDATES

13.1. Vendors release firewall upgrades and version updates for many security reasons, importantly some are to combat vulnerabilities and loopholes in outdated hardware and software.

13.2. You must patch the firewall's operating system and application software with the latest security patch at least every six months, or in response to a risk raised through vulnerability management.

13.3. Vulnerability tests must be conducted on firewalls to assess hardware or software for flaws and weaknesses.

13.4. Internet facing firewalls must have a full ITHC at least annually.

14.0 ADDITIONAL BEST PRACTICE

14.1. The following controls are additional requirements to consider to ensure firewalls are configured for optimal effectiveness.

14.2. You must change the default firewall administrator or root password – please refer to the Trust's Password Policy (CP74) to identify password minimum requirements.

14.3. For physical firewalls, you must ensure that physical access to the firewall is controlled.

14.4. You must backup the firewall rule base and configuration files at least every 6 months, and before and after any changes are made.

14.5. Firewalls must be implemented and configured to operate resiliently in case of hardware or physical environment failures.

14.6. Firewalls must synchronise to a central time source

14.7. A record should be kept of all rules, this must include the business approver, explanation of business need and the expected configuration and activity of each rule.

15.0 REFERENCE OTHER DOCUMENTATION

15.1. The following documents should be read in conjunction with this Policy and its associated procedural guidelines:

- CP59 Data Protection and Confidentiality Policy
- CP74 Password Policy

END