# Network Firewall Implementation Policy

## Overview

Firewalls are hardware devices or software programs that control the flow of traffic between networks, servers, and computer systems. They protect internal resources from intrusion and are an important part of information security. This policy defines the policies and procedures around firewall implementation within the [LEP].

## Purpose

This policy helps protect [LEP] information asset availability, confidentiality, and integrity from outside intrusion and hacking activities. Firewalls and the technology/procedures that support them help protect internal networks and manage traffic in and out of the network.

## Scope

This policy applies to all [LEP] staff responsible for managing premise, physical, and logical networks as well as internet and application security.

## Policy

[LEP] uses a multi-layered approach to protect computer resources and assets. Network security design shall include firewall functionality at all places in the network where outside exploitation exposures exist. This may include areas other than the network perimeter to provide an additional layer of security and protect devices that are placed directly onto external networks (de-militarized zone).

### Management Responsibilities

The [Insert Appropriate Role] or their designee shall ensure the following controls are in place:

* A formal process for approving and testing all network connections and changes to the firewall and configurations
* Current network infrastructure diagrams identifying connections between environments containing sensitive data and other networks, including any wireless networks
* Network diagrams and documents detailing sensitive data flows across systems and networks
* Firewalls are positioned at each Internet connection and between any demilitarized zone (DMZ) and the internal [LEP] network
* Documentation is in place that describes groups, roles, and responsibilities for management of network components
* Documentation exists for use of all services, protocols, and ports/services allowed
* Procedural review of firewall configurations at least annually
* A standard configuration exists for fast and consistent firewall deployment
* All critical firewalls are identified and are under maintenance/replacement contracts
* Subscriptions/licenses satisfy business and legal requirements

### General Configuration

The [Insert Appropriate Role] or their designee shall define how an organization’s firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization’s information security policies. [LEP] IT staff shall:

* Restrict inbound and outbound traffic to that which is necessary for sensitive data and specifically deny all other traffic
* Install perimeter firewalls between any all wireless networks and sensitive data and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment and environments containing sensitive data
* Regularly review and develop a list of the types of traffic needed by the organization and how they must be secured including an analysis shall include which types of traffic can traverse a firewall under what circumstances
* All inbound and outbound traffic not expressly required shall be blocked which reduces the risk of attack and also decreases traffic volume carried on the [LEP]’s internal network
* Identify configuration requirements when determining firewalls
* Consider network related assets as well as the firewall technologies most effective at blocking network related threats
* Identify performance considerations and concerns surrounding firewall integration into existing network and security infrastructure
* Design firewall solution design to include [LEP] physical network requirements as well as consideration of possible future needs
* Create network traffic rules that are as specific as possible while allowing user functionality
* Document traffic and protocol exceptions a firewall may need for use in management and administrative functions
* Implement a demilitarized zone (DMZ) that limits inbound traffic to system components that provide authorized publicly accessible services, protocols, and ports/services
* Disallow direct connections (inbound and outbound) for traffic between the internet and environments containing sensitive, confidential, or personally identifiable information
* Implement anti-spoofing measures to detect and block forged source IP addresses from entering the internal network
* Use stateful packet inspection technologies (e.g dynamic packet filtering) so that only established connections are allowed into the network
* Ensure all system components that store sensitive information (e.g. production databases) in an internal network zone are segregated/segmented from the DMZ and other untrusted or public networks
* Disallow private IP addresses and routing information to unauthorized parties
* Authorized methods to obscure IP addressing shall include Network Address Translation (NAT) configurations, removal or filtering of route advertisements for private networks, and internal use of RFC1918 address space instead of registered addresses
* Formal hardening and testing procedures are in place. As part of the hardening procedure, default passwords and configurations shall be changed to further enhance device security
* All device passwords shall be long and complex meeting all requirements in the [LEP] Access Control and Password policy
* Enterprise firewalls shall be under maintenance and support contract with appropriate response time guarantees

### Administration and Management

The [Insert Appropriate Role] and network support staff are responsible for managing firewall architectures, policies, software, and other solution components. Policy rules shall be updated as [LEP] network and access requirements change, when new applications or servers are implemented within the network, or should other business drivers indicate. The following firewall management procedures shall be implemented:

* Performance shall be monitored to ensure availability and operation of all premise and architectural firewall components
* Monitoring and alerting tools shall be used to proactively monitor and address issues before the environment has an outage or a threat is detected
* Configuration rules and policies shall be managed by a formal change management control process
* Rules, reviews, and periodic tests shall be performed to ensure continued compliance with organizational policy
* Software and hardware firmware shall be patched as vendors provide updates to address vulnerabilities
* All configurations shall prohibit direct internal access to public networks (e.g. Internet)
* Port or Internet Protocol (IP) address filtering technology shall be used to limit network access
* Configurations shall restrict all traffic, inbound and outbound, from untrusted wired/wireless networks and hosts and specifically deny all other traffic except for necessary protocols
* Physical access to hardware firewall devices shall be tightly restricted to authorized security and network personnel
* All desktops, laptops, and similar devices should have software firewalls installed as an additional means of protection
* Firewall security log files shall be configured, maintained, and periodically reviewed for anomalies
* Logs shall be of sufficient size to provide useful information in case of a security event
* Appropriate security staff shall receive periodic training regarding new and developing threats, current data security practices, and changes in compliance regulations

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [LEP] internal operational processes and procedures. Examples of appropriate controls and management practice include:

* Formalized change procedures surrounding network configuration and management
* Archival logs of configuration changes and premise intrusion monitoring
* Network system documentation and regular review processes
* System and device patching logs
* Historical incident and response logs

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff responsible for managing and supporting the [LEP] production network.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 8/30/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |