# Firewall Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

[Company Name] operates perimeter firewalls between the Internet and its private internal network in order to create a secure operating environment for [Company Name]’s computer and network resources. A firewall is just one element of a layered approach to network security. The purpose of this Firewall Policy is to describe how [name firewall] firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of access for business users.

The Firewall Policy is subordinate to [Company Name]’s general Security Policy, as well as any governing laws or regulations.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Firewall Policy refers specifically to the [name firewall] firewall. The role of this firewall is to [describe role and relevant features]. The firewall will (at minimum) perform the following security services:

* Access control between the trusted internal network and untrusted external networks.
* Block unwanted traffic as determined by the firewall rule set.
* Hide vulnerable internal systems from the Internet.
* Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
* Log traffic to and from the internal network.
* Provide robust authentication.
* Provide virtual private network (VPN) connectivity.

All employees of [Company Name] are subject to this policy and required to abide by it.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

## Policy

The approach adopted to define firewall rule sets is that all services will be denied by the firewall unless expressly permitted in this policy. The [firewall name] firewall permits the following outbound and inbound Internet traffic.

* Outbound – All Internet traffic to hosts and services outside of [Company Name]. [Insert any other relevant information.]
* Inbound – Only Internet traffic from outside [Company Name] that supports the business mission of [Company Name] as defined by [name of individual or policy]. [Insert any other relevant information.]

The table below identifies the most common services used for Internet communications within the [Company Name] environment. For each service type, the table will indicate whether the firewall will accept it, accept it with authentication, or reject it.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Traffic/Service** | **Port** | **Outbound  (internal to external)** | **Inbound  (external to internal)** | **Inbound VPN  (secure VPN to internal)** | **Comments** |
| DNS |  |  |  |  |  |
| Finger |  |  |  |  |  |
| FTP |  |  |  |  |  |
| gopher |  |  |  |  |  |
| HTTP |  |  |  |  |  |
| ICMP |  |  |  |  |  |
| IMAP |  |  |  |  |  |
| LDAP |  |  |  |  |  |
| NFS |  |  |  |  |  |
| NNTP |  |  |  |  |  |
| NTTP |  |  |  |  |  |
| POP3 |  |  |  |  |  |
| TFTP |  |  |  |  |  |
| Telnet |  |  |  |  |  |
| NFS |  |  |  |  |  |
| NetBIOS |  |  |  |  |  |
| RPC |  |  |  |  |  |
| Rsh |  |  |  |  |  |
| SMTP |  |  |  |  |  |
| SNMP |  |  |  |  |  |
| SSH |  |  |  |  |  |
| X Windows |  |  |  |  |  |
| [Insert service] |  |  |  |  |  |
| [Insert service] |  |  |  |  |  |

[Department name] is responsible for implementing and maintaining [Company Name] firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and one designee. Password construction for the firewall will be consistent with the strong password creation practices outlined in [Company Name]’s Password Policy.

Any questions or concerns regarding [firewall name] firewall should be directed to [staff member name/contact information].

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

* [Company Name] employees may request changes to the firewall’s configuration in order to allow previously disallowed traffic. A firewall change request form, with full justification, must be submitted to the IT department for approval. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.
* [Company Name] employees may request access from the Internet for services located on the internal [Company Name] network. Typically, this remote access is handled via a secure, encrypted virtual private network (VPN) connection. [Describe VPN type and capabilities here.]
* VPN sessions will have an absolute timeout length of [insert time length]. An inactivity timeout will be set for [insert time length]. At the end of these timeout periods, users must re-authenticate to continue or re-establish their VPN connection. A VPN connectivity request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed.
* From time to time, outside vendors, contractors, or other entities may require secure, short-term, remote access to [Company Name]’s internal network. If such a need arises, a third-party access request form, with full justification, must be submitted to the IT department for approval. Approval is not guaranteed.
* Turnaround time for the above stated firewall reconfiguration and network access requests is approximately [insert number] days from the receipt of the request form.
* Firewall logs will be backed up [insert frequency] and archived [insert frequency]. Firewall logs will be reviewed [insert frequency].

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |