NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor
Raja Sambandam
Acting Cabinet Secretary & State CIO

Policy Title:	**Firewall Policy**
Policy Number:	**DoIT-361-706**
Effective Date:	**03/21/22**
Issued By:	**DoIT CIO**
Distribution:	**DoIT IT Resource Users**
Approved by:	**Raja Sambandam, Acting Cabinet Secretary**

1. AUTHORITY

Pursuant to the New Mexico Department of Information Technology Act, NMSA 1978, § 9-27-1 *et seq.*, the Secretary of the Department of Information Technology (DoIT or Department) shall exercise general authority over all department employees, manage all operations of the Department, and administer and enforce the laws with which the Secretary or the Department is charged.

Pursuant to NMAC 1.12.20, DoIT is responsible to implement network controls to maintain security in its trusted, internal network, and to ensure the protection of connected services and networks.

2. PURPOSE

This document describes DoIT's official Policy regarding firewall configuration, implementation, and management, and establishes base configuration standards and guidelines surrounding the support and setup of all DoIT firewall devices. Firewalls are a critical security asset to protect DoIT's information resources. All firewalls are required to be configured, implemented, and maintained in a standardized and secure fashion.

3. SCOPE

This Policy applies to all DoIT firewalls used in DoIT's production and non-production environments,and to the network security administrators who service them and DoIT associated managers.

4. DEFINITIONS

a. **DoIT IT Resource Users -** All DoIT employees, contractors, vendors, and other users of DoIT information technology (IT) resources.

b. **DMZ –** Data Management Zone is a physical or logical sub-network that contains and exposes DoIT's external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to provide an additional layer of security to DoIT's local area network.

c. **Firewall –** A part of a computer system or network designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer-based applications based upon a set of rules and other criteria.

d. **Production Network** – The network used for DoIT's daily business, the impairment of which would result in direct loss of functionality for DoIT IT Resource Users and/or customers.

e. **Non-production Network –** Any network used solely for testing, development, training, or other non-production purposes. Any network that is stand-alone or firewalled off (segmented) from the production network(s) and whose impairment would not cause direct loss to DoIT noraffect the production network.

5. POLICY

Configuration standards are to be developed and documented to ensure consistency and proper management of rule sets to maintain the security and integrity of firewalls at the Department. DoIT follows a deny-by-default approach to network traffic. All connections between internal networks and the non-trusted networks are required to incorporate an approved firewall and routing access controls. DoIT network security teams are responsible for maintaining network diagrams, including any virtual system components. Such diagrams must depict the firewalls and ingress/egress points.

a. **Configuration Standards and Minimum Requirements:**

i. Secure and harden the underlying operating system of all firewall components, enabling only the required services for firewall operation.

ii. Remove all non-essential networking or system services from the firewall.

iii. Implement for the network layer, wireless networks, Web applications at the application layer, or any connection between the trusted and untrusted zones at theDMZ.

iv. Keep firewall software and systems current with new system releases, upgrades and patches.

v. Apply all patches according to the DoIT Patching and Updating Policy and Change Management Policy and process.

vi. Any traffic that is not explicitly allowed will be dropped according to the cleanup rule at the end of the firewall rule set.

vii. Document all allowed services, protocols, and ports, including security features implemented for those protocols considered to be insecure with formal tracking with business reason and management approval.

viii. Clearly define and document firewall rules. Rules will pass only required traffic to allow the services between necessary systems to operate. Rules set to “Any – Any” are prohibited unless approved by the DoIT Chief Information Security Officer (CISO) or Chief Information Officer (CIO) designee.

ix. Obtain approval of any changes to the firewall configurations or rules inaccordance with the DoIT Change Management Policy and process.

x. Store logs of all changes to firewall configuration parameters, enabled services, and permitted connectivity in a centralized location as approved by CISO or CIO designee. Daily logphysically and logically protected area for at least one year from timestamp. At least 3 months of logs are to be immediately available.

xi. Protect DoIT internal RFC 1918 address space from unauthorized disclosure.

xii. Use only approved firewall products compatible with the DoIT IT architecture withinDoIT’s network.

xiii. Store all firewall devices in access restricted areas (under lock and key) only accessible by authorized personnel (Staff approved by the agency CIO).

xiv. If firewall layer-7 capabilities are used, layer-7 rule sets inspections occur after allprevious layer rules based on network/IP addresses have been processed.

xv. Firewall policies shall be configured to accept only inbound and outbound data traffic which is required based on business needs; all other data traffic should be denied.

xvi. Firewall policies shall take into account the source and destination of the traffic in addition to the content.

xvii. Data traffic with invalid or private addresses shall be default blocked from delivery.

xviii. Proposed modifications to network and security equipment must be requested and approved for implementation through the agency change management procedure.

xix. To prevent unauthorized modifications of the firewall configuration, the firewall administrator must review the firewall configuration quarterly.

xx. Any form of cross-connection, which bypasses the firewall, is strictly prohibited.

xxi. Remote firewall administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access.

xxii. Details of firewall, and security devices type, software versions, and configuration data will not be disclosed without the permission of the agency CIO.

b. Firewall Logging, Monitoring and Audit Processes:

i. Before introduction to any network, enable and maintain firewall audit andsystem logs for all firewall systems to support monitoring and investigations into network activities.

ii. Document reviews of firewall logs daily, at a minimum, to ensure that the firewalls are operating in a secure manner and to identify security issues. Reviews are required to be signed by reviewer and timestamped.

iii. Alarm or monitoring tools must alert Network Security Administrators and managers (Network Security Manager or Agency CIO) of security-related events originating from a firewall.

iv. Logging minimum standards mandate recordation of source and destination, date and time, service and/or port, URL, and attempted access to the network service.

v. Collect configuration tracking changes made during a login session.

vi. Backup firewall policies and configurations monthly, at a minimum, and store in an access restricted area under lock and key.

vii. Review of firewall rules is required every 6 months, at a minimum, to ensureunauthorized changes have not been made, and that rules are still effective and appropriate.

c. Firewall Administration Minimum Requirements:

i. Create individual accounts for each administrator/user; no shared or generic accounts are allowed. Groups, containing permissions based on common responsibilities for firewall access, are required as a primary control for access. Place individual accounts within appropriate groups and do not apply permissions at the individual user level.

ii. Remove or deactivate vendor default credentials or common administrator account.

iii. All passwords are required to adhere to DoIT's Password Policy.

iv. Privileges to modify firewall functionality, connectivity, and/or services are required to be restricted to designated individuals with a business need for these privileges. Accessand permission rights to firewalls administration are to be approved by the network security manager. For every firewall, at least two knowledgeable DoIT staff members, adequately trained to make changes as required, must have access for logical management.

v. All administrative access to firewalls is required to operate via secured protocols. Any remote access, if allowed, requires two-factor authentication.

6. ROLES AND RESPONSIBILITIES

a. DoIT CISO

The DoIT CISO or CIO designee will ensure development, implementation, documentation, updates, and distribution of information necessary to ensure the security of firewall and firewall type appliances.

b. DoIT Network Security Administrators

DoIT Network Security Administrators must adhere to the Firewall Policy when making any changes to a firewall device, reviewing daily logs, and maintaining up-to-date ruleset documentation. Network Security Administrators must also enforce appropriate firewall reporting. Such firewall reports must include firewall usage, list of administrators and their access rights, list of rules for audit, list of services and ports, select security issues from logs, etc.

7. EXCEPTIONS

The DoIT CISO must approve any exceptions to this Policy in writing.

8. VIOLATIONS OF POLICY

Any DoIT IT Resource User found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

9. REFERENCES

a. 1.12.20 NMAC

b. National Institute of Standards and Technology SP800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*

c. National Institute of Standards and Technology SP800-53 r4: AC-4, AC-6, CM-3, CM-6, SI- 3, **SI-4, SC-7, SC-28**

d. International Organization for Standardization/International Electrotechnical Commission 27002:2013: 12.6.1, 13.1.2, 13.1.3

e. Information Systems Audit and Control Association: *Controls Objectives for Information and Related Technologies v5.0*

10. CHANGE HISTORY

Date	Version	Changed By	Change Comments
09/30/2019	1		Initial Draft
09/30/2020	2		Revision Draft
02/26/2021	3	Raja S	Revised and routed for Union approval
05/13/2021	4	Olga Serafimova	Reviewed and revised for legal compliance
12/28/2021	5	Brenda Fresquez	Reviewed for quality assurance
3/15/22	6	Marko Satarain	No changes, reviewed and accepted by HR—Marko Satarain, Legal—Todd Baran and CWA—Dan Secrist

Approval

DocuSigned by:
437214FBE82C453...

3/21/2022

Raja Sambandam, Acting Cabinet Secretary

Date