State of New Mexico Statewide
Architectural Configuration Requirement
Title: Firewall Functionality Standard
N-STD004.001
Effective Date: October 18, 2005

1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act NMSA, 9-27-1 et. seq. (1978).

2. Purpose

This standard defines the required functionality and configuration of firewalls on the State of New Mexico Enterprise network. This standard is developed to increase the security of the Enterprise network and associated business systems and services. The standard allows for centralized log reading, improved response, and invoking of appropriate action to address security threats.

3. Scope

This applies to all Executive Agencies and to any other Agency or Entity utilizing Executive
Agency infrastructure.

The Department Secretary or Agency Director, working in conjunction with the Department or Agency Chief Information Officer (CIO) or IT Lead, shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each agency.

This standard implements the following:

- Centralized log reading by creating common supported platforms and firewall applications;
- Reduced incident response time to security breaches;
- Improved log reading methodology;
- Improved overall firewall procedures for both the core and agency networks;
- Established best practices on standardized equipment;
- Supported Computer Security Incident Response team (CSIRT) by providing consistent configuration standards;
- Improved Enterprise Network Management in the event of a major security threat.

4. Standard

Physical/ Facilities/ Installation

- High availability must include UPS (un-interruptible power supplies) and/or generator backup. A redundant power source should be used wherever available. Dedicated power circuits are required.
- All firewall devices will be stored in a secured network location.

Minimum Hardware

- Firewalls must be physically configured (sizing) at time of purchase to support agency needs for three years. For example, if a business function requires gigabit speed within three years, a 100-megabit platform would be insufficient to meet business needs.
- New or existing firewalls must include a maintenance strategy. Hardware must have an appropriate plan for spare parts replacement and or contractual support. Maintenance Agencies must present to DoIT the support plan upon time of purchase.
- The number of supported simultaneous VPN connections must exceed the projected growth. For example, if a VPN is expected to grow to greater than 100 users, a VPN that only supports 50 users would be insufficient to meet business needs.
- Firewall devices that require high availability must have dual power supplies or run in a fail-over configuration. High availability is required on core devices and at aggregation points.

Configuration

- Firewall devices must support secure management communication.
- All firewall devices will be held to access level security standards as defined in the approved state password policy.
- *VPN* Compatibility must be supported if multiple vendors are used. Compatibility must be demonstrated prior to purchase.
- Firewalls may only be entered into DNS, provided a secured view of the router is developed. DNS Standards define.
- Firewalls must support an audit trail to track changes. New firewall configurations will be updated after all changes. After all firewall configuration changes are completed, backup will be completed and stored in a secure network location.
- *Configuration*. Default and final rules must be 'Deny All.'

Restrictions

- The Enterprise Service Provider; DoIT will have the authority to isolate or disconnect any agency network that has been identified as a viable security threat to the Enterprise Network. The Enterprise Service Provider; DoIT will notify the Agency of its intention to shut the Agency network down and document the specific reasons for doing so. The Agency will have sufficient time to identify the cause and source of the threat and disable or resolve the threat at the agency level. If the threat has not been resolved within the specified time, the Enterprise Management Group will have the right to isolate or disconnect the Agency's network until such time as the security threat is resolved.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

None

7. Attachments

None

8. Version Control

N-STD-004.001

9. Revision History

Original 04/25/05
Revised 10/18/05
Format Updated 09/18/13