Idaho Technology Authority (ITA)

ENTERPRISE POLICIES – P4500 SECURITY - COMPUTER AND OPERATIONS MANAGEMENT

Category: S6050 – FIREWALL SECURITY

CONTENTS:

I. Definition
II. Rationale
III. Approved Standard(s)
IV. Approved Product(s)
V. Justification
VI. Technical and Implementation Considerations
VII. Emerging Trends and Architectural Directions
VIII. Procedure Reference
IX. Review Cycle
X. Contact Information
Revision History

I. DEFINITION

See ITA Guideline G105 (Glossary of Terms) for any definitions. G105-ITA Glossary of Terms

II. RATIONALE

Firewalls shall block all inbound and outbound traffic that has not been explicitly permitted by the firewall policy—traffic that is not needed by the organization. This practice, known as deny-by-default, decreases the risk of attack and can also reduce the volume of traffic carried on the organization's networks. Because of the dynamic nature of hosts, networks, protocols, and applications, deny-by-default is a more secure approach than permitting all traffic that is not explicitly forbidden. A coordinated firewall approach is necessary to monitor, track, and restrict access to portions of the network.

III. APPROVED STANDARD(S)

NIST SP 800-30 (Most current)

NIST SP 800-41 (Most current)

IV. APPROVED PRODUCTS(S)

Refer to approved state contracts for IT Security Products:
https://purchasing.idaho.gov/statewide-contracts/

V. JUSTIFICATION

With the ITS maintaining a set of registered firewall security products purchased from the State Contract, the State exercises secure supply chain accountability and can continue to leverage its buying power and position itself for the future possibility of an enterprise security architecture and shared infrastructure.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

The deployment, configuration and management of a firewall is a complex task requiring skilled resources. Agencies shall ensure the appropriate skill sets are available to implement and maintain a firewall system.

Basic principles that organizations follow in the planning of firewall deployments include:

- **Integrate Zero Trust principles**. Zero Trust emphasizes that no user, device, or network segment is inherently trusted, regardless of its location within the enterprise environment. When planning firewall deployments, organizations should design rule sets, network segmentation, and access controls based on the assumption that threats may already exist inside the network. This includes enforcing least-privilege access, validating all traffic explicitly, and continuously monitoring firewall activity to ensure that trust is never assumed and is always verified.

- **Use devices as they were intended to be used.** Firewalls shall not be constructed of equipment not meant for firewall use. For example, routers are meant to handle routing, not highly complex filtering, which can cause an excess burden on the router's processor. Additionally, firewalls shall not be expected to provide non-security services, such as acting as a web server or email server.

- **Create defense-in-depth**. Defense-in-depth involves creating multiple layers of security. This allows risk to be better managed, because if one layer of defense becomes compromised, another layer is there to contain the attack. In the case of firewalls, defense-in-depth can be accomplished by using multiple firewalls throughout an organization, including at the perimeter, in front of sensitive internal departments, and on individual computers. For defense-in-depth to be truly effective, firewalls shall be part of an overall security program that also includes products such as anti-malware and intrusion detection software.

- **Pay attention to internal threats.** Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders but can involve internal hosts infected by malware or otherwise

compromised by external attackers. Important internal systems shall be placed behind internal firewalls.

- **Document the firewall's capabilities.** Each model of firewall has different capabilities and limitations. These will sometimes affect the planning of the organization's security policy and firewall deployment strategy. Any features that positively or negatively affect this planning shall be written into the overall planning document.
- **Logging and alerts**. Logging is a critical step in preventing and recovering from failures as well as ensuring that proper security configurations are set on the firewall. Proper logging can also provide vital information for responding to security incidents. Whenever possible, the firewall shall be configured both to store logs locally and to send them to a centralized log management infrastructure. Resource constraints, firewall logging capabilities, and other situations may impair the ability to store logs both locally and centrally.

A successful firewall deployment can be achieved by following a clear, step-by-step planning and implementation process. Firewall planning and implementation phases, including:

1. **Plan.** The first phase of the process involves identifying all requirements that an organization will consider when determining which firewall to implement to enforce the organization's security policy.

2. **Configure**. The second phase involves all facets of configuring the firewall platform. This includes installing hardware and software as well as setting up rules for the system.

3. **Test.** The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment. The primary goals of testing are to evaluate the functionality, performance, scalability, and security of the solution, and to identify any issues—such as interoperability—with components.

4. **Deploy**. Once testing is completed and all issues are resolved, the next phase focuses on deployment of the firewall into the enterprise.

5. **Manage**. After the firewall has been deployed, it is managed throughout its lifecycle to include component maintenance and support for operational issues. ITA Guideline G535 (Firewall Configuration Guideline) identifies the industry configuration and deployment best practices that should be leveraged by agencies implementing their internal firewalls. ITA Guidance G536 Firewall Change Request should be followed by agencies requesting policy changes to the State managed perimeter firewall.

Firewall Review – A firewall review should be conducted every six (6) months to validate security configurations.

The firewall review should include:

- Review/Update Network Diagram

- Rule Sets
- Update Information Flow Diagrams
- List of Deficiencies
- Remediation Plan of Action and Milestones.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

The industry continues to move toward more distributed and adaptive security architectures that integrate layered defense-in-depth with Zero Trust principles. Modern enterprise environments increasingly rely on firewalls deployed not only at the perimeter but also across endpoints, remote locations, and internal network segments. This shift supports continuous verification, granular access control, and improved isolation of systems, allowing organizations to better manage evolving threats within complex hybrid environments.

VIII. PROCEDURE REFERENCE

ITA Enterprise Guideline G535 (Firewall Configuration Guidelines)
ITA Enterprise Standard S6040 (Firewall Change Request)

IX. REVIEW CYCLE

Every 3 years

X. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.
To report an incident, send email to cyber@its.idaho.gov or call (208) 605-4000.

REVISION HISTORY

05/05/26 – Creates a new firewall security standard by relocating requirements from P4570, clarifying procurement and Zero Trust expectations, and standardizing technical sections and review requirements.

Effective Date: May 5, 2026