Idaho Technology Authority (ITA)

ENTERPRISE POLICIES – P4500 SECURITY - COMPUTER AND OPERATIONS MANAGEMENT

Category: P4570 – 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

Firewall: A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.
Ruleset: A set of directives that govern the access control functionality of a firewall. The firewall uses these directives to determine how packets should be routed between its interfaces.

II. RATIONALE

Generally, firewalls should block all inbound and outbound traffic that has not been expressly 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 (Revision 1)
NIST SP 800-41 (Revision 1)

IV. APPROVED PRODUCTS(S)

Organizations are required to purchase firewall appliances from the State Security Contract. In addition, organizations requesting to install a firewall that is not registered with the Office of IT Services (ITS), Executive Office of the Governor, must complete a comprehensive risk analysis to be reviewed and approved by the ITS Chief Information Security Officer (CISO).

Organizations can send the comprehensive risk analysis for review to security@its.idaho.gov.

V. JUSTIFICATION

With the ITS maintaining a set of registered firewall security products purchased from the State Security 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 should ensure the appropriate skill sets are available to implement and maintain a firewall system.

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

- **Use devices as they were intended to be used.** Firewalls should 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 should 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 should 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 should 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 should 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 should 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 should 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 G5XX Ports, Protocol, and Services 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 is evolving towards a layered “defense in depth” approach to the firewall architecture. Desktop, remote PC, laptop, and local office/agency firewalls are a few of the components being more broadly implemented as part of enterprise security systems.

VIII. PROCEDURE REFERENCE

ITA Enterprise Guideline G535 (Firewall Configuration Guidelines)
ITA Enterprise Guideline G536 (Firewall: Ports, Protocols, and Services Request)

IX. REVIEW CYCLE

Six (6) Months

X. CONTACT INFORMATION

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

REVISION HISTORY

07/01/18 – Changed “OCIO” to “ITS”.

02/23/16 – This policy replaces Enterprise ITA Standard S3200 (Firewall-Security) and provides high-level direction to state agencies regarding hardening and security best practices.

07/01/13 – Changed “ITRMC” to “ITA”.

06/16/09 – Added Procedure Reference and deleted Timeline.

04/25/05 – Added Cisco Firewall products.

Effective Date: October 2, 2001