Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G535 Firewall Configuration Guidelines

CONTENTS:

I. DEFINITIONS

Demilitarized Zone (DMZ): An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.

Deny by Default: To block all inbound and outbound traffic that has not been expressly permitted by firewall policy.

Firewall: A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Network Address Translation (NAT): A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema.

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

Agencies shall deploy firewall mechanisms in the DMZ to control access to the State's network backbone and/or routed infrastructure. Protective controls shall at a minimum include the following:

1. Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.

2. Authentication to ensure that routing tables do not become corrupted with false entries.

3. Network address translation (NAT) to screen internal network addresses from external view.

4. Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the agencies.

III. GUIDELINE

Firewall Configuration and Installation

1. The default firewall policy is to deny by default, meaning all ports to be closed. Only those ports for which an agency has written, documented business reasons for opening shall be open.

2. Each agency shall establish a process for evaluating policy changes and rulesets that, at a minimum, incorporates requirements to comply with NIST 800-41 best practices.

3. All agencies shall designate a minimum of two (2) authorized firewall administrators. At least one of the designated firewall administrators will be a security specialist who is consulted before firewall policy changes are approved and implemented.

4. Block all ports then permit specific ports which have a business requirement access while incorporating additional hardening as necessary to have a comprehensive security policy.

5. For temporary or emergency port openings, the agency process shall establish a maximum time for the port to be open, which shall not exceed 10 working days. The agency authorized firewall policy administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.

6. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.

7. Firewalls shall be installed in locations that are physically secure from tampering. The agency Information Security Coordinator (ISC) shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the agency security liaison.

8. Firewall rules sets shall always block the following types of network traffic:

    - Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.
    - Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.
    - Traffic inbound to the State Network containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter with the following exceptions: To allow testing initiated from internal IT support groups, ICMP echo replies and ICMP TTL expired will be permitted inbound to the State Network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter, for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping.
    - Inbound network traffic containing IP Source Routing information.
    - Inbound or outbound network traffic containing a source or destination address of 0.0.0.0
    - Inbound or outbound network traffic containing directed broadcast addresses.

9. Minimum Firewall Requirements:

    - Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages.
    - Local accounts shall be configured to only become active when the device cannot make contact with the central unit. During normal operation, the local account exists but is unusable.
    - Firewalls must use an authentication mechanism that provides accountability for the individual.
    - Passwords on firewalls shall be kept in a secure encrypted form.

10. Monitoring and Filtering:

    - Logging features on state network firewalls shall capture all packets dropped or denied by the firewall, and agency staff or the entity managing the firewall shall review those logs at least monthly.
    - Each agency's firewall policy shall be reviewed and verified by agency staff at least quarterly.

IV. PROCEDURE REFERENCE

NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

NIST SP 800-41 (Revision 1) (Guidelines on Firewalls and Firewall Policy)

Enterprise ITA Policy P4570 (Firewall Security)

Enterprise ITA Policy P4140 (Cybersecurity Framework)

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

V. 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

07/01/2018 – Changed “OCIO” to “ITS”.

Effective Date: December 15, 2015