State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.04.01	Border Security	D	07/13/2022	1 of 4

1.0 PURPOSE

This standard is established to enhance the protection of agency internal networks through secure network firewalls and intrusion prevention systems (IPS).

2.0 SCOPE

This standard applies to all state agencies meeting the criteria identified in the State Information Security Program Policy, Section 1.2 Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

NRS 205, Crimes Against Property
NRS 603A, Security and Privacy of Personal Information
State Information Security Program Policy, 100
Suspension of Services, S.2.05.02
Secure Software Configuration, S.6.02.01
Software Patch Management, S.6.03.01
Malware Defenses, S.6.08.01

6.0 STANDARD

This standard enforces a ‘defense in depth’ approach that creates the need for multiple controls to protect internal systems.

6.1 Firewalls

A firewall system must be used at a site’s dedicated connection to the Internet and between connections with other untrusted networks.

A. Firewall Systems

1. Agencies deploying firewall systems shall have a firewall administrative policy describing authorized and unauthorized use of their firewall system.

2. All firewall systems must fail in a closed state, not allowing any traffic to pass.

3. Firewall systems must be certified using common criteria by an independent reviewer.

4. Firewalls shall have the ability to support complex access control for transit traffic in any direction.

5. IPv6 must be disabled on all firewall devices if the protocol is not in use.

B. Packet Capture

Firewalls must be capable of capturing relevant packet data for analysis and forensics.

C. System Management

1. The firewall administrator shall be formally trained in the secure configuration and management of their system.
2. System administrators shall test their systems by performing periodic, non-destructive scans and other checks to detect security vulnerabilities, expected response and errors in configuration.
3. System administration features or privileged functions must be restricted to authorized administrators. Administrators must use secure protocols (cryptography) when not physically connected to the device.
4. All configuration changes must use a formalized change management process..
5. Separate test environments should exist to test configuration changes and code upgrades prior to deployment. When the upgrade is to repair a critical vulnerability or the test environment is not capable of representing the complexity of the production environment or adequately testing the conditions necessary, this at the discretion of the agency.
6. Configurations must be reviewed for unnecessary and incorrect data at least quarterly.

6.2 Intrusion Prevention Systems (IPS)

A. IPS scans or response features shall not be directed at untrusted network nodes or directed at trusted nodes outside of their administrative domain without prior written approval.

B. Automated response to malicious events consisting of blocking traffic to State of Nevada resources, dropping traffic or manipulating content is permitted under the guidelines of Standard S.2.05.02 Suspension of Services.

7.0 DEFINITIONS

ACLs (Access Control Lists): An access control list is a group of statements that defines a pattern that would be found in an IP packet. Incoming packets are then scanned for a pattern that matches one defined in the list. A permit or deny rule associated with the pattern, determines whether the packet is allowed to continue to its destination or not.

Border Security: Security measures designed and implemented on systems, appliances and devices that face the Internet.

Common Criteria: The Common Criteria for Information Technology Security Evaluation, international standard (ISO/IEC 15408)

Complex access control: Able to manipulate traffic by source or destination address, protocol, or port or any combination of those identifiers in any direction.

Firewall system: A firewall system can be any device specifically engineered to shield a site, subnet or individual computer from protocols and services that can be abused from hosts outside the secure area of the business. Firewalls are usually located at a site’s connection to the Internet, but may also be located to provide protection for a smaller collection of hosts, a single host, or subnet which has access to external networks.

Formally trained: Technicians and staff who have received advanced training in system, appliance or devices management from the vendors or certified third parties.

NAT (Network Address Translation): NAT translates between the internal address and the assigned registered internet address.

Trusted Nodes: A node that is within the boundaries of an administrative domain (AD) and is trusted in the sense that the admission control requests from such a node do not necessarily need a policy decision point (PDP)(RFC 2753).

8.0 RESOURCES

SilverNet Security Classifications, EITS Security Standard E.5.04.01

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by SISC	3/31/2022
State Chief Information Security Officer (CISO)	Signature on File	6/30/2022
State Chief Information Officer (CIO)	Signature on File	7/13/2022

Document History

Revision	Effective Date	Change
A	2/22/2018	Major Revision, rewrite of old standard
B	12/26/2018	Renumbering (128 to S.5.04.01) and compliance to ADA standards
C	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)
D		Review and update, in coordination with CIS Control IG2 review