State of Nevada

Information Technology Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
4.63	A	Network Perimeter Defense	05/09/02	1 of 4

1.0 PURPOSE

The Network Perimeter Defense Standard is established for the protection of an agency's internal network from unauthorized access.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

4.0 RESPONSIBILITIES

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

5.0 RELATED DOCUMENTS

State IT Security Policy 4.02
State Information Security Officer (ISO) Roles and Responsibility, 4.03
NIST – National Institute of Standards and Technology, Special Publication 800 Series.

6.0 STANDARD

A network perimeter defense system implements administrative policies that define the services that may be accessed, and control the access that is allowed to a protected network. It implements network access controls by forcing connections to pass through the firewall gateway, where they can be examined and evaluated.

6.0.1 FIREWALLS

A firewall is an organization's first line of defense against attacks that form from the outside. The best security policy approach implements a "defense in depth" approach that does not rely on a single application or piece of hardware for its functionality.

A firewall system must be used at a site's dedicated connection to the Internet and 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) This policy shall be an extension of the organizational policy regarding the protection of information resources in the organization.

3) The firewall system shall have the ability to support a “deny all services except those specifically permitted” design.

4) No untrusted node shall be allowed to initiate a connection to an internal node.

5) The firewall system shall have the ability to support ACLs (Access Control Lists).

B. Advanced authentication mechanisms

The firewall system shall contain advanced authentication features.

C. Packet Filtering

The IP filtering language shall filter on as many attributes as possible, including source and destination IP address, protocol type, source and destination TCP/UDP port, and inbound and outbound interface.

D. Logging

The firewall system shall contain the ability to log traffic.

E. Operating Systems

1) If the firewall system requires an operating system such as UNIX, a secured version of the operating system shall be part of the firewall, with other security tools as necessary to ensure firewall host integrity.

2) The firewall system administrator shall install current security patches for the operating system.

F. Stateful Inspection

A stateful inspection firewall system must be used for high traffic Internet access or enterprise networks.

G. NAT (Network Address Translation)

The firewall system shall be able to take advantage of NAT for increased network security.

H. System Management

1) The firewall system administrator shall be formally trained to harden their systems to guard against intrusion.

2) The system administrator shall develop and adhere to procedures for the installation of patches and security fixes.

3) The system administrators shall test their systems by performing periodic, non-destructive scans and checks of host systems to detect common vulnerabilities and errors in configuration.

6.0.2 Server Security

All servers shall be evaluated for hardening requirements and evaluation results documented.

6.0.3 Intrusion Detection Systems

A. Intrusion detection systems (IDS) shall not seriously impede the flow of traffic within an internet work, and must have management consoles or administrative consoles/plug-ins to monitor and manage the system.

B. IDS scans or features shall not be directed at untrusted network nodes, or directed at trusted nodes outside of the administrative domain without prior written approval.

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 it's destination or not.

Firewall system - A firewall system can be a router, a personal computer, a host or a collection of hosts, set up specifically to shield a site, subnet or individual computer from protocols and services that can be abused from hosts outside the organizational structure. 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.

Hardening a system - The process of hardening is that of identifying exactly what a specific machine will be used for and removing or disabling all system components not necessary for that function. Hardening may be treated as any and all of the steps used to improve the security on a computer. This often includes limiting the user population, password policies, access controls, user and group rights, and intrusion detection.

NAT (Network Address Translation) - NAT translates between the internal address and the assigned internet address. It provides network security as a by-product of the translation process. Through translation, NAT hides the internal network IP addresses so that external parties only see the external address.

Stateful Inspection - A stateful inspection firewall system keeps a state-table of connections whereby it monitors the state of a TCP connection and allows traffic accordingly. It does content checking by passing protocols through a validation exercise. It can handle network address translation, and authenticate connections. It parses UDP through a set of rules and expected responses.

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) decision (RFC 2753).

Untrusted Nodes – see trusted nodes.

8.0 EXCEPTIONS/OTHER ISSUES

Request for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

Approved By		
Title	**Signature**	**Date**
State IT Security Committee Chair	Signature on File	12/19/2001
NV IT Operations Committee Chair	Signature on File	05/09/2002
Governor/Governor's Representative	Signature on File	06/17/2003

Document History		
Revision	**Date**	**Change**
(-)		Initial release.