

	Georgia Technology Authority	
Title:	Network Security - Boundary Protection	
PSG Number:	SS-08-047.01	Topical Area: Security
Document Type:	Standard	Pages: 4
Issue Date:	3/31/08	Effective Date: 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	To establish requirements for agencies to implement network boundary protection strategies.	

PURPOSE

Controlling the flow of information into and out of the internal operational network and protecting it from malicious insiders, external entities with malicious intent, intentional or inadvertent denial of service attacks and unauthorized access or disclosure of sensitive information are essential activities of network security. Boundary or perimeter protection measures provide protection and monitoring capabilities against these and other threats to the network. Effective design, installation, configuration and maintenance of network boundary protection mechanisms are critical tasks in providing effective network security.

This standard establishes requirements for agencies to implement network boundary protection strategies.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

Agencies shall establish controls that monitor and control the flow of information within and at the external boundary of the information systems and networks they operate.

Business Owners shall designate an individual (e.g. Agency ISO, CTO etc) responsible for managing and administering network boundary protection strategies (e.g. firewalls and other boundary protection devices).

Boundary Protection strategies shall include but are not limited to:

Physical Security: Agencies shall employ due diligence in ensuring physical security at any location where boundary protection devices are installed.

Title:	Network Security-Boundary Protection
--------	--------------------------------------

Access Control: All access to state information systems and networks shall be controlled and monitored in accordance with all enterprise access control policies and standards.

Interconnections: All connections to information systems outside the security boundary of an agency's information system or the state backbone (internet, or other external network or information system) shall be fully documented, authorized, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) and be continuously monitored.

Least Functionality: Network boundary control devices shall be configured to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services. Agencies shall also monitor for inappropriate use of network services.

Default Denial: Agency firewalls shall block every network connectivity path and network service not explicitly authorized by the Agency ISO.

Configuration Changes and Documentation: All changes to firewall configuration parameters, enabled services, and permitted connectivity shall be authorized by the designated security manager, and documented in accordance with change control policies and procedures. Privileges to modify the functionality, connectivity, configuration and services supported by firewalls shall be restricted to the designated firewall administrator(s); Agency ISO and/or other authorized designee(s).

Firewall Monitoring and Logs: Agencies shall continuously monitor boundary protection devices for suspicious activity and inappropriate use, and utilize the firewall logging capabilities in accordance with the log management policies and standards.

Denial of Service; intrusion detection and malicious code: Agencies shall ensure boundary protection controls protect and monitor the network against malicious code, denial of service, intrusions, and other hacking attacks. Systems categorized as MODERATE or higher shall alert parties responsible for monitoring or responding when these suspicious conditions exist.

Record Retention: All documentation and/or firewall logs shall be retained in accordance with each agency's respective retention policies and schedules. No specific retention requirements are set forth by these Standards.

Periodic Review: Firewall configurations shall be reviewed to ensure compliance to agency or State security policies. Supporting documentation shall exist for all enabled services. Agencies are responsible for testing their firewall configurations for effectiveness.

Effective Date:	March 31, 2008	2 of 4
-----------------	----------------	--------

Title:	Network Security-Boundary Protection
--------	--------------------------------------

Security Updates: Agency personnel responsible for managing firewalls will subscribe to security advisories and other relevant sources providing up-to-date information about firewall vulnerabilities and apply relevant patches, updates and/or other recommended protective actions.

Contingency Planning: Agencies shall take appropriate measures to ensure that operational failures of boundary protection mechanisms do not result in unauthorized releases of information outside the information system boundary. Firewall configurations shall be backed up fully, a redundancy and failover strategy shall be employed and alternate processing sites shall provide the same levels of protection as the primary site.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Network Security-Information Flow (Policy)
- Network Access and Session Controls (Standard)
- Web and E-Commerce Security (Standard)
- Change Control Standard
- Malicious Code Standard

REFERENCES

NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
NIST SP 800-94 Guideline to Intrusion Detection and Prevention Systems

TERMS and DEFINITIONS

Information System (hereafter referred to as 'system') - A discrete set of information resources (workstations, servers, applications, network, etc) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System Boundary – All the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and people).

Boundary Protection (or perimeter defense) – Tools and techniques used to manage, control and protect the security objectives of information stored, processed and transmitted within and between network boundaries; such as but not limited to controlled interfaces, intrusion detection, anti-virus, network forensic analysis, log monitoring.

Controlled Interfaces - Mechanisms that facilitate the adjudication of different

Effective Date:	March 31, 2008	3 of 4
-----------------	----------------	--------

Title:	Network Security-Boundary Protection
--------	--------------------------------------

interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).

Note: The PSG number was changed from S-08-047.01 on September 1, 2008

Effective Date:	March 31, 2008	4 of 4
-----------------	----------------	--------