IT 17.04: Firewall Management Standards

Policy Authority

BTS Administrative Rule 2.01- Security Administrative Rule
BTS Administrative Rule 2.16- Firewall Security and Management

Purpose

Firewalls provide a perimeter defense mechanism to limit the City's exposure to external threats which may damage the City's information technology systems. Effective management of these devices requires procedures on the authorized use and modification of these devices.

Policy

These devices are managed by the Information Security Office. The Information Security Office engineers, and approves all standards, configurations and rules changes related to the City's firewalls.

Procedure

In order to accomplish the aforementioned policy, certain firewall management procedures must be established including:

- Scope
- Roles and Responsibilities
- Firewall Change Types
- Schedule & Process
- Process Exceptions

Scope
These procedures cover any Bureau of Technology Services managed firewall

Roles and Responsibilities
Information Security evaluates and implements changes to the City's firewalls and firewall management console. The Information Security Office engineers, maintains, and approves all standards, configurations and rule changes related to the security of the City's firewall platform. All decisions related to engineering and standards are determined by Information Security in consultation with Network Engineering. Information Security prioritizes, tests and approves any patches or firmware upgrades.

Firewall Change Types
There are two types of firewall changes:

- Abbreviated changes
- Full changes

Abbreviated changes are limited to change(s) in:

- The Internet Protocol (IP) address of the affected device, or
- Predetermined access control list changes, or
- Proxy exceptions

These types of changes are expected to have limited consequences on the overall security posture of the City's network and therefore can be implemented without Information Security approval. In all case, Information Security will audit

the overall security of the change, regardless of whether it is an abbreviated or full change.

Full changes are all other types of firewall changes. These changes require a full change control form to be completed and approved by Information Security before such changes are implemented. The necessary information to process a full change is located within IT 17.04.01 Firewall Management Procedures.

Schedule & Process

Schedule
Information Security reviews and approves changes on a weekly basis. Once these changes are approved, they are forwarded for implementation based on the schedule listed below.

Given the duties described above, certain service level agreements exist to ensure the timely delivery and secure management of the City's firewalls. These service level agreements include the following timelines:

Action	Delivery Timeline
-Rule Changes	
Abbreviated	2 business days
Full	7 business days
-Zone Migration	7 business days
-Patch/Firmware Implementation	30 calendar days from vendor release
-Configuration Change	5 business days

These timelines apply only for completed requests. Completed requests are those requests that provide all necessary information outlined in IT 17.04.01 Firewall Management Procedures and are entered into Altiris, the City's ticketing system.

Process
Table 1 below describes the process. The description provided below is designed to include more detailed information about this table.

Step #1 (Change Control Ticket Creation)
The appropriate party (Network Engineering and Support, Server Support, etc.) shall complete the appropriate change control ticket and review it with Information Security for completeness and approval. Requesting parties should work with either Information Security to provide any necessary information. Altiris is the tool for submitting change requests. The necessary information to create a change control ticket is located within IT 17.04.01 Firewall Management Procedures.

Step #2 (Vulnerability Assessment)
The security posture of both abbreviated and full changes must be evaluated. In order to accomplish this, Information Security utilizes a security checklist to determine the relative safety of a change. This checklist is based on the National Institute of Standards and Technology's (NIST) *Guidelines to Securing Public Web Servers*, Special Publication 800-44 version 2.[1]

Table 1: Security Checklist

	Requirement

[1] National Institute of Standards and Technology, *Guidelines to Securing Public Web Servers*, Special Publication 800-44 version 2, September 2007, http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

☐	Fully Patched Operating System
☐	Fully Patched Applications
☐	Active and Updated Anti-Virus Software
☐	Utilizes internal Network Time Protocol (NTP), Domain Name Services (DNS), WINS
☐	Password Policies Match BTS Administrative Rule 2.05
☐	Unnecessary Services Are Removed

Information Security ensures that security requirements are met by conducting initial and ongoing Nessus vulnerability scans. If this vulnerability scan identifies areas of concern rated as higher than a 5, the affected change will require immediate rollback and remediation.[2] Such scans will only find vulnerabilities in "network" services. They will have no visibility into local vulnerabilities or configuration settings. Penetration tests will be conducted as needed for high risk environments.

Step #3 Change Implementation and User Notification

Information Security implements all firewall changes. Once a user's change has been reviewed (approved or denied), Information Security shall notify the user of the decision. In those cases where the change has been denied, Information Security shall work with the user to identify the security issue as well as any known "fix" for the issue.

Process Exceptions

In order to maintain current service levels at the Portland Police Bureau, certain exceptions to the above standards are warranted. Specifically, the Bureau of Technology Services' (BTS) Police Information Technology Division (ITD) is responsible for rule changes within the City's firewall platform that services the Portland Police Bureau. Police ITD also utilizes the City's central firewall management console for purposes of logging and managing these rule changes.

All other standards listed above continue to apply to Police ITD including policies surrounding patches and upgrades, the change control process, and vulnerability assessments. Additionally, Police ITD should utilize the aforementioned security checklist to assess the safety of its rule changes.

Information Security provides vulnerability assessments of these firewalls and provides Police ITD with information necessary to remediate any critical vulnerability that is revealed as part of this assessment.

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Logan Kleier, Information Security	BTS Leadership Team	3/13/09
1.1	8/3/09	Logan Kleier, Information Security	BTS Leadership Team	7/10/09

[2] According to Tenable Security, Nessus rates their vulnerabilities via CVSS (Common Vulnerability Scoring System). CVSS scores are rated on a 1 to 10 scale. Tenable Security translates a CVSS score of 7-9 as a "High" security risk and 10 is rated as a "Critical" risk.