IT 17.04.1: Firewall Management Procedures

Policy Authority

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

Purpose

In order to maintain compliance with various security regimes such as Payment Card Industry- Data Security Standard (PCI-DSS), the Bureau of Technology Services (BTS) is required to document its management procedures for its access control devices such as routers and firewalls. These procedures include a clearly documented firewall rule-set. A clearly documented firewall rule-set allows for a regular review of these rules to ensure the validity and necessity of any traffic that traverses BTS' access control devices.

This document augments and clarifies BTS's IT Standard 17.04: Firewall Management Standards by providing an operational guide for firewall management.

In addition to the compliance issues, there are a variety of reasons that access control device rules cannot be approved in a "blanket" fashion. These reasons include:

- Separation of duties and;
- Need for Risk Analysis

Procedure

In order to accomplish the aforementioned policy, certain firewall management procedures must be established. The implementation details of these procedures are defined below.

Pre-approved rules

BTS's IT Standard 17.04 references a group of abbreviated changes that are "predetermined access control list changes". The following defines what these predetermined changes are.

System management rules

For every new zone created, a group will also be created that contains all of the hosts within the zone to allow access to system management services such as DNS.

The following groups will exist:

- bts_web_mgmt_update_servers_grp containing AltirisNS, BTSWUS, City16
- bts_rose_time_servers_grp containing the approved time servers
- bts_rose_dns_servers_grp containing the approved Domain Name Service (DNS) servers
- bts_app_syslog_servers_grp containg the approved Syslog servers
- bts_app_snmp_servers_grp containing the approved Simple Network Management Protocol (SNMP) servers

The following rules are approved for every zone

- <zone_host_group> -> bts_web_mgmt_update_services_grp, allow HTTP, HTTPS
    - This rule will allow Windows updates, McAfee Electronic Policy Orchestrator (EPO) updates, and Altiris inventory services.
- <zone_host_group> -> bts_rose_time_servers_grp, allow NTP (UDP/123)
- <zone_host_group> -> bts_rose_DNS_servers_grp, allow DNS (TCP53 & UDP/53)
    - These rules will allow DMZ hosts to access DNS and time services.
- <zone_host_group> -> bts_app_syslog_servers_grp, allow Syslog (UDP/514)
- bts_app_snmp_servers_grp -> <zone_host_group>, allow Simple Network Management Protocol (SNMP) (TCP & UDP 161,162)
- <zone_host_group> -> bts_app_snmp_servers_grp, allow Simple Network Management Protocol (SNMP) (TCP & UDP 161,162)
    - This rule will allow Syslog and SNMP system management protocols for centralized logging and performance monitoring

Only the needed backup protocols are approved. This may be implemented using a DSClient[1] with Asigra or using a DSClient to use Common Internet File System (CIFS) to transfer files. Either of these two rules are approved (but not both). The 2nd (using CIFS) is preferred because the risk to the Asigra servers is less.

- <host> -> Asigra server, allow TCP/4401
- Asigra DSClient -> <host>, allow TCP/445 (CIFS)

The following rules are approved for networking devices. This will support centralized networking devices management functions.

- Network_Admin -> <network_device>, allow PING & Secure Shell (SSH)
- bts_app_snmp_servers_grp -> <network_device>, allow SNMP
- <network_config_backup_server> -> <network_device>, allow SSH
- <network_device> -> bts_app_snmp_servers_grp, allow SNMP
- <network_device> -> bts_app_syslog_servers_grp, allow SYSLOG
- <network_device> -> bts_rose_time_servers_grp, allow NTP
- <network_device> -> <acs servers>, allow (Terminal Access Controller Access- Control System) TACACS (TCP/49)

[1] DSClient – Asigra is the backup solution the City has implemented. As part of that solution, a DS-Client is used to move data to a primary DS-System. This DS-Client design then backups a certain amount of hosts/servers.

Other pre-approved rules

- Host IP address changes
    - When a host has been assigned a new IP address (server or desktop), modifying the firewall object to reflect the new IP address is approved. This does not include new servers, server replacements, or server redesigns. When a server is brought online (regardless of it being a replacement for an existing server) all firewall rules must be approved by BTS Information Security before implementation (except those listed above) since the secure posture of the server needs to be analyzed.
- Proxy changes
    - Since changes to the proxy exception list pose little risk, these are pre-approved though still require documentation and review by BTS Information Security after the change has been made.

Firewall documentation process

Purpose

The purpose of the Change Management documentation is to clearly articulate the nature and impact of any changes to access control devices. Such documentation is integral in understanding historical choices as well as performing both internal and external audits.

Change management request process

Firewall changes must be documented within BTS's Altiris helpdesk solution with an Altiris ticket number generated for every requested change. By using this ticket number within the firewall configuration, it will allow firewall rules to be quickly and consistently traced back to the ticket which explains their business need. It also allows for an identification of undocumented rules or objects (anything without a ticket number). When tickets are ready for review they should be assigned to the "BTS Security" Altiris queue.

Required information

When tickets are created within the Altiris helpdesk system, the following information is required. Please link tickets when appropriate as well. A ticket template will exist with the following fields. When a ticket has already been created, please use the following information to modify the ticket to bring it inline with our needs.

- Set "Type" to "Request"
- Set "Title" to "Firewall Rule Request: [Description]"
- Set "Category" to "Services" -> "Firewall"
- Set "Assigned" to "BTS Security"

- Assign the requester as the "Contact"
- Title should reflect the fact it is a firewall change and

Field	Required	Description
Devices Affected	Both (abbreviated and full)	What access control devices will require modification to meet the request? Also, include which devices will be used to filter or process the traffic. You may select multiple devices.
Termination Date	When applicable	When can the rule, policy, or other work be removed?
Type of Request	Yes	Is this a new request or a modification to an existing request? If it is a modification, be sure to link related tickets.

Type of Change	Both	What type of work is being done and what type of policy is affected?
Business Need	Both	What is the business need behind the change? This needs to include enough information so that someone who is only semi-familiar with the City's environment can understand why the change was made and who is impacted.
Is sensitive data involved?	Both	Is any personally identifiable information involved in this request such as names and social security numbers or medical information? Are there any credit or debit card numbers involved?
Requesting Bureau/Department	Both	Who is requesting the change and who can be contacted about the change? This would also include contacting them in the future to confirm the policy is still required.
External traffic	Both	Will this change implement a policy allowing traffic to flow into and/or out of the City's network?
Access Policies (address & port)	Both	Using this field, document what access policies need to be modified in "human readable" terms. Include source and destination addresses as well as ports. Object and group names may be used but please include their definition when the object or group name is not obvious. You may use an excel spreadsheet to do this for large requests.
Other Changes	When applicable	Use this field to document any other changes that are being made to fulfill the request.
Applications Affected	When applicable	This field is used for documenting any applications that may be affected by the change, either internal or external.
Supporting Documents	When applicable	Any documents or diagrams that help others to understand the nature and impact of the request.

Approval Sources

Information Security requires authorization from the supervisor or manager responsible for services or devices involved in a firewall change. The Service Level Agreement listed in IT 17.04 apply in those change requests where Information Security can secure the non-BTS employees understanding and acknowledgement of any risks associated with proposed rule changes. This understanding and acknowledgment does not take the place of Information Security approval. It only serves as an additional approval layer to ensure Bureau understanding of security risks.

Conventions for Object Naming

- *Any group, host or service will have "_grp" appended to the name*
- Rules (policies within the Juniper interface)
  - The helpdesk ticket number will be documented within every rule using the "Name" field. Other descriptive words may be used as the implementers' discretion.
- Address object/group
  - The naming convention will follow <bu>_<hostname>_<type>_<description> where
    - <bu> is the business unit (bureau or subgroup within bureau). If the object is from BTS, this may be ignored.
    - <hostname> is the assigned host name for the device. If hostname is descriptive and includes other fields, the other fields may be ignored.
    - <type> consists of the following (which may be combined)
      - Virtual machine (vm)

- web server (web)
- application server (app)
- file server (fs)
- database (db)
- general server (serv)
- desktop (desk)
- external (ext)

- <description> is used to quickly describe the purpose of the host object
- Examples include sap_sapdpi_db_devpi, sapppi_prodpi, cgisfile, bts_city16_app_antivirus

- The “comment” field will be used to document the ticket number when the object is first created.

- Service object/group
  - The naming convention will follow <protocol>_<port>_<description> where
    - <protocol> is Transmission Control Protocol (TCP), Uniform Datagram Protocol (UDP), or TCPUDP for both
    - <port> is the service port number or common name (HTTP, HTTPS, SSH)
    - <description> is a short description of what the service is for
  - The “comment” field will be used to document the ticket number when the object is first created. The “comment” field is not available within the web interface for custom service objects, thus can only be documented from the NSM.
- Zones
  - The naming convention will follow <bu>_<type>_<description> where
    - <bu> is the business unit (bureau or subgroup within bureau). If there is no single bureau using the zone, this may be ignored.
    - <type> is of
      - External (ext) – allowing internet access
      - Internal (int) – only allowing intranet access
      - Virtual Machine Guest (vmg) – append this to the types above if a VMware DMZ
    - <description> may contain the purpose of the DMZ or other descriptive language

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Logan Kleier, Information Security Manager	Logan Kleier, Information Security Manager	3/13/09