Baltimore City Community College

*Changing Lives...Building Communities*

**Date:** January 19, 2011

**Title of Procedures:** Firewall Security

---

**Procedures (check one): New ___X___ Revised _____**

**Applies to (check all that apply):**

**Faculty ____ Staff__ Students ___**

**Division/Department: ___ College__X__**

**Topic/Issue**:

To establish an understanding of the function that a firewall plays in the overall security of BCCC's network.

**Background to Issue/Rationale for Procedure**:

The Baltimore City Community College (BCCC), Computer Information Technology Services (CITS) manages a perimeter firewall between its Internet connection and the BCCC campus network to establish a secure environment for the campus' network and computer resources. This firewall filters Internet traffic to mitigate the risks and potential losses associated with security threats to the campus network and information systems.

**State/Federal Regulations Requirements (cite if applicable)**:

State of Maryland, Department of Information Technology Security Policy and Standards

**Procedure Language**:

The firewall administrators examine the Firewalls' log activities on a regular basis. Network engineers periodically review the configuration of the firewall to confirm that any changes to the configuration are legitimate. The current configuration has been established:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic.
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. For reference purposes, RFC 1918 reserves the following address ranges for private networks:
  10.0.0.0 to 10.255.255.255 (Class A)
  172.20.0.0 to 172.50.255.255 (Class B)
  192.168.0.0 to 192.168.255.255 (Class C)
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
- Inbound traffic containing IP Source Routing information.
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (localhost).
- Inbound or Outbound network traffic containing a source or destination address of 0.0.0.0.
- Inbound or Outbound traffic containing directed broadcast addresses.

The firewall should block all inbound traffic unless that traffic is explicitly needed for inbound server connections. The following services and applications in addition to the previous rules should be configured at a minimum with any exceptions noted:

| Application | Port Numbers | Action |
|---|---|---|
| **Login Services** | | |
| | FTP – 21/tcp | restrict with strong authentication |
| | NetBIOS – 139/tcp | always block |
| | r services – 512/tcp – 514/tcp | always block |
| **RPC and NFS** | | |
| | Portmap/rpcbind – 111/tcp/udp | always block |
| | NFS – 2049/tcp/udp | always block |
| | lockd – 4045/tcp/udp | always block |
| **NetBIOS in Windows NT** | | |
| | 135/tcp/udp | always block |
| | 137/udp | always block |
| | 138/udp | always block |
| | 139/tcp | always block |
| | 445/tcp/udp in Windows 2000 | always block |
| **Windows** | 6000/tcp – 6255/tcp | always block |

**Naming Services**

| | |
|---|---|
| DNS – 53/udp | restrict to external DNS servers |
| DNS zone transfers – 53/udp | block unless external secondary |
| LDAP – 389/tcp/udp | always block |

**Mail**

| | |
|---|---|
| SMTP – 25/tcp | block unless external mail relays |
| POP – 109/tcp and 110/tcp | always block |
| IMAP – 143/tcp | always block |

**Small Services**

| | |
|---|---|
| ports below 20/tcp/udp | always block |
| time – 37/tcp/udp | always block |

**Miscellaneous**

| | |
|---|---|
| tftp – 69/udp | always block |
| finger – 79/tcp | always block |
| NNTP – 119/tcp | always block |
| NTP – 123/tcp | always block |
| LPD – 515/tcp | always block |
| syslog – 514/udp | always block |
| SNMP –161/tcp/udp,162/tcp/udp | always block |
| BGP – 179/tcp | always block |
| SOCKS – 1080/tcp | always block |

**ICMP**

block incoming echo request (ping and Windows traceroute)
block outgoing echo replies, time exceeded, and destination unreachable messages except “packet too big” messages (type 3, code 4

## Firewall Access Controls:

**Note:** Firewall access should be submitted **at least a week** in advance of the day that service is required.

***Procedures for Requestor***:

1) Firewall Access requests must be submitted to the CITS Service Desk (CSD).
   a) The request must be submitted in one of the following ways:
      - Customers should call the CITS Service Desk at 410-462-7420.
      - Customers should email their requests to helpdesk@bccc.edu

2) The CSD staff assigns the request to the Firewall Administrator.

***Procedures for Firewall Administrator***:

3) The Firewall Administrator obtains the following information from the vendor or requestor:

- Application name
- Client application name
- The name of the organization hosting the service
- Technical support contact information
- Phone number
- Destination IP address (single or multiple)
- Communications' Protocol ID (TCP and/or UDP)
- Begin date and time or use
- End date and time of use

4) The firewall administrator evaluates the information and does the following:

a) If the information provided is satisfactory and in compliance with BCCC's Network Policy, the service request is approved.

b) If the information provided is not satisfactory and not in compliance with BCCC's Network Policy, the service request is rejected.

c) The Firewall administrator should contact the vendor or requestor to inform them why the service request was rejected and relay what additional information should be obtained in order to reverse the rejection.

5) The firewall administrator closes the service request upon completion.

**Proposed Implementation Date:** March 1, 2011

**Proposed by:** **Mohan Sharma**
**Vice President/Senior Staff Member**

**Approved by the Board of Trustees:** March 22, 2011

**Originator/Division:** CITS/President's Office