**Introduction**

One of the information technology priorities for Old Dominion University (ODU) is to provide and maintain a safe secure computing environment. The Office of Computing and Communications Services (OCCS) manages multiple perimeter firewalls between its Internet connections and the University campus network providing the first level of defense against security threats to the University's network and information technology resources. OCCS maintains routers and switches that provide a robust and redundant network environment for academic, administrative, and research University communities.

**Purpose**

The purpose of this standard is to establish an understanding of the function that a router or switch plays in the overall security of ODU’s network in documenting the configuration, maintenance, and monitoring of enterprise-wide router technology used to safeguard the University's information technology resources.
Standard Statement
All OCCS managed routers and switches at ODU must follow this standard. Departures from this standard will be permitted only if approved in advance and in writing by the Assistant Director of Communications Services.

Conceptually, ODU’s enterprise network technology divides the campus network into multiple layers. Each layer represents a different level of trust/protection. By enforcing a degree of separation between the layers, the firewalls and routers help prevent unauthorized access from a less trusted layer to a more trusted layer. From the inner most to the outer most, the layers are:

- core layer
- distribution layer
- access layer

Border routers are used to provide security between the Internet and the University; access and distribution layer routers provide connectivity to the end stations. The core and distribution routers must have a redundant failover unit to provide service continuity should the primary unit fail. The router access control lists enforce specific security or business requirements. Access to the University's perimeter and/or internal network(s) will be based on parameters such as (but not limited to):

- Application/service use such as public, administrative, student only, internet only, etc
- IP address and port
- Outbound connections (more trusted to less trusted layer) are generally permitted by default
- Inbound connections (less trusted to more trusted layer) are denied by default.

Given the nature of the University’s academic environment, the border routers cannot be configured to typical industry accepted standards (i.e. complete deny by default posture). ODU’s border routers do not constrict all unnecessary traffic; it is open to all traffic and denies as needed

Due to the requirements of high bandwidth and reduced latency, core routers do not inspect network traffic via access control lists. Distribution routers are utilized for specific traffic filtering and quality of service bandwidth management

Access layer switches provide layer two connectivity from end-stations to the distribution layer and are not utilized for any security filtering.

Due to individual security needs, depending on the type of information to be protected, the following information should be used to maximize the security of the network environment.

The following type of network traffic should always be blocked:

- Inbound traffic from a non-authenticated source system with a destination address of the router system itself.
- Inbound traffic with a source address indicating that the packet did not originate from the access layer subnet.
- 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 at the border router. For reference purposes, RFC 1918 reserves the following address ranges for private networks:

  10.0.0.0 to 10.255.255.255 (Class A)
  172.16.0.0 to 172.31.255.255 (Class B)
  192.168.0.0 to 192.168.255.255 (Class C)

Additional blocked inbound networks

  169.254.0.0
  192.0.2.0
  255.0.0.0

- Inbound traffic containing Simple Network Management Protocol (SNMP) traffic except for specific network management stations.
- 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.

Border Router Configuration – Blocked Services

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Service</th>
<th>Port(s) (transport)</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>swipe</td>
<td>137 (tcp &amp; udp)</td>
<td>Netbios-ns</td>
</tr>
<tr>
<td>54</td>
<td>narp</td>
<td>138 (tcp &amp; udp)</td>
<td>Netbios-dgm</td>
</tr>
<tr>
<td>55</td>
<td>mobile</td>
<td>139 (tcp &amp; udp)</td>
<td>Netbios-ssn</td>
</tr>
<tr>
<td>57</td>
<td>skip</td>
<td>161 (tcp &amp; udp)</td>
<td>snmp</td>
</tr>
<tr>
<td>77</td>
<td>Sun-nd</td>
<td>162 (tcp &amp; udp)</td>
<td>snmp-trap</td>
</tr>
<tr>
<td>99</td>
<td>Encrypt method</td>
<td></td>
<td></td>
</tr>
<tr>
<td>171</td>
<td>reserved</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User Distribution Router Configuration – Blocked Services
User distribution routers are used to provide network traffic routing, validate source ip addresses from end stations, and security standard enforcement on a subnet-by-subnet basis.

Server Distribution Router Configuration – Blocked Services
The server distribution routers are used in conjunction with firewalls to protect the campus main servers including mail servers, web servers, and database servers from the internet and other parts of the campus. The routers are used to provide network traffic routing, validate source ip addresses from end stations, and security standard enforcement on a subnet-by-subnet basis.

Router configurations should be backed up to the configuration servers with the end of each change session. The configuration server backups should be internally situated backup mechanism, e.g., tape drive.

Logs
The routers will be configured to use system logging (syslog) to export its log messages to designated syslog servers. The router logs will be backed up and archived in accordance with current practices implemented on the syslog server. The routers will be configured to only accept SNMP requests from specific network management devices. At a minimum, the router log will be configured to detect:

1. Emergencies, such as unusable messages
2. Alert, critical conditions, error and warning messages
3. Logon access and configuration attempts made to the firewall

Router log activity, and router administrators examine the logs on a regular basis. The network time protocol (NTP) will be used to synchronize the logs with other logging systems such as intrusion detection. In addition to examining the logs, the Information Security Officer or his/her designee periodically reviews the configuration of the firewall to confirm that any changes made are legitimate.

Router/Switch Physical Security
All Old Dominion University router and switches must be located in locked rooms accessible only to those who must have physical access to such routers and switches to perform the tasks assigned by management.
Responsibilities

The Information Security Officer is responsible for ensuring the implementation of the requirements of the router standards. Daily operation and maintenance of the router will be the responsibility of the Assistant Director of Communications Services.

Employees who violate this standard may be subject to disciplinary action. Anyone who knows or has reason to believe that another person has violated this standard should report the matter promptly to his or her supervisor or the Information Security Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person reporting a violation of this standard will itself be considered a violation of this standard that may result in disciplinary action.

Change Management

The system owner of a system located on a restricted subnet may request via a FootPrints ticket (or email if Footprints is unavailable), a router access control list (acl) change to allow (inbound connections) from a system on a less trusted network.

1. Temporary/testing access requests must include a reasonable expiration date not to exceed 30 days at a time.
2. Systems supporting access from the public internet (e.g. web and mail servers) will be scanned for vulnerabilities and approved by OCCS Security before firewall “rules” will be modified.

The Assistant Director of Communications Services or his/her designee must approve in writing all configuration changes and rule requests. Changes will not be approved if the University determines them to be a threat to the confidentiality, integrity, or availability of its information technology resources and systems.

Immediate emergency router acl changes to stabilize a network infrastructure situation such as an attack or compromise can be made as required with written notification to the Assistant Director of Communications Services.

Router configurations will be reviewed annually or when there are major changes to the network requirements that may warrant significant changes to the router. Examples of such situations are (but not limited to):

1. The implementation of major enterprise computing environment modifications
2. Any occurrence of a major information security incident
3. When new applications are being considered. Alternatively, when an application is phased out or upgraded, the firewall configuration should be formally changed where appropriate.

Operational Procedure

For any service that needs to be open to the public, OCCS requires a vulnerability scan of the server. The server administrator will be required to fix all major and critical security problems before the OCCS Security Team will approve the request.

All router acl requests must come from the system owner. Please review the ACL Request Procedures document.

To place a router acl request, open a Footprints ticket. If Footprints is unavailable, please email your request to abuse@odu.edu.

Please follow the diagram below before placing a router rule modification request.
Old Dominion University
Router Request Work Flow
(last updated: 20080303)

Have a business need that requires access campus resources from Internet?

- A small group of employees
- Vendor or contractors
- Students with granted exception
- Many employees and students
- Large amount of students
- Entire internet community

Get authorization For request

Request approved by system owner?

- yes
  - Private Server
    - Discuss with OCCS security Team about opening VPN or router ticket
      - yes
        - VPN supported services
          - Open vpn ticket
      - no
        - Limited source IP addresses allowed on border router
          - Server admin receives scan report and fixes problem, then request another scan
            - no
              - Pass scan?
                - no
                  - Server admin receives scan report. OCCS security team finish router acl request
                - yes
                  - Server admin receives scan report. OCCS security team finish router acl request