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 a firewall in each distribution to provide authenticated network access in open computing environments. Additional firewalls are maintained in support of specialized functions.

Purpose

The purpose of this guide is to establish an understanding of the function that a firewall plays in the overall security of ODU’s network and document the configuration, maintenance, and monitoring of enterprise-wide firewall technology used to safeguard the University's information technology resources.
Policy Statement

All OCCS managed firewalls at ODU must follow this standard. Departures from this standard will be permitted only if approved in advance and in writing by both the Information Security Officer and Assistant Director of Communications Services.

Conceptually, ODU’s enterprise firewall technology divides the campus network into multiple layers/networks. Each layer represents a different level of trust/protection. By enforcing a degree of separation between the layers, the firewall helps prevent unauthorized access from a less trusted layer to a more trusted layer. From outermost (least trusted/protected) to innermost (most trusted/protected), the layers are:

- Internet and other external IP networks
- Perimeter networks (varies according to level of trust)
- Internal network (most trusted/protected networks)

Security between the Internet and the University will be maintained by a firewall. The firewall must have a redundant failover unit to provide service continuity should the primary unit fail. The firewall will inspect packets and sessions to determine if the traffic should be permitted or denied. 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 firewall cannot be configured to typical industry accepted standards (i.e. complete deny by default posture). ODU’s border firewall does not constrict all unnecessary traffic; it is open to all traffic and denies as needed. The research network border firewall is configured to completely deny by default posture and requests to allow sourced outside traffic are reviewed on a case-by-case basis.

Perimeter firewalls are deployed in each of the user distribution modules to provide authenticated network connectivity via non-University maintained computing systems (e.g. laptops). Stateful inspection of network traffic protection is provided within the firewall unit.

Inner layer firewalls provide protection for specialized applications and are generally configured to in a deny by default environment. Stateful inspection of network traffic protection is provided within the firewall unit.

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 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)
  172.16.0.0 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.
• 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.

Perimeter Firewall Configuration – Blocked Services

<table>
<thead>
<tr>
<th>Port(s) (transport)</th>
<th>Service</th>
<th>Port(s) (transport)</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (udp)</td>
<td>reserved</td>
<td>4444 (tcp)</td>
<td>W32/Blaster</td>
</tr>
<tr>
<td>7 (tcp &amp; udp)</td>
<td>echo</td>
<td>5000 (udp)</td>
<td>UPNP</td>
</tr>
<tr>
<td>9 (tcp &amp; udp)</td>
<td>discard</td>
<td>5900 (tcp)</td>
<td>VNC</td>
</tr>
<tr>
<td>19 (tcp &amp; udp)</td>
<td>chargen</td>
<td>6129 (tcp)</td>
<td>Dameware</td>
</tr>
<tr>
<td>25 (tcp)</td>
<td>smtp *</td>
<td>6346-6347 (tcp &amp; udp)</td>
<td>Gnutella</td>
</tr>
<tr>
<td>42 (tcp &amp; udp)</td>
<td>nameserver</td>
<td>8998 (udp)</td>
<td>W32/Sobig.f@MM</td>
</tr>
<tr>
<td>69 (tcp &amp; udp)</td>
<td>tftp</td>
<td>9100 (tcp)</td>
<td>HP Jetdirect</td>
</tr>
<tr>
<td>80 (tcp)</td>
<td>www *</td>
<td>13000 (tcp)</td>
<td>W32.Spybot</td>
</tr>
<tr>
<td>111 (tcp &amp; udp)</td>
<td>sunrpc</td>
<td>17300 (tcp &amp; udp)</td>
<td>Kuang2_the_virus</td>
</tr>
<tr>
<td>135 (tcp &amp; udp)</td>
<td>loc-srv</td>
<td>27374 (tcp)</td>
<td></td>
</tr>
<tr>
<td>137 (tcp &amp; udp)</td>
<td>Netbios-ns</td>
<td>31337 (udp)</td>
<td>Back Orifice</td>
</tr>
<tr>
<td>138 (tcp &amp; udp)</td>
<td>Netbios-dgm</td>
<td>59980 (tcp)</td>
<td></td>
</tr>
<tr>
<td>139 (tcp &amp; udp)</td>
<td>Netbios-ssn</td>
<td>65000 (tcp)</td>
<td>Stacheldraht</td>
</tr>
<tr>
<td>161 (tcp &amp; udp)</td>
<td>snmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>162 (tcp &amp; udp)</td>
<td>snmp-trap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>235 (tcp)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>444 (tcp)</td>
<td>Simple network paging protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>445 (tcp &amp; udp)</td>
<td>microsoft-ds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>515 (tcp)</td>
<td>lpr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>520 (udp)</td>
<td>rip</td>
<td></td>
<td></td>
</tr>
<tr>
<td>524 (tcp &amp; udp)</td>
<td>Novell Directory Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>593 (tcp)</td>
<td>Dcom msrpc/blaster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>666 (tcp)</td>
<td>Doom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>901 (tcp)</td>
<td>Samba/SWAT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>995-999 (udp)</td>
<td>pop3s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1214 (tcp)</td>
<td>Kazaa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1433 (tcp)</td>
<td>MS SQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1444 (tcp)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1761 (tcp &amp; udp)</td>
<td>sms-helpdesk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1900 (udp)</td>
<td>MS Windows messenger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1993 (udp)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3
<table>
<thead>
<tr>
<th>Port(s) (transport)</th>
<th>Service</th>
<th>Port(s) (transport)</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>2049 (udp)</td>
<td>NFS</td>
<td>2222 (tcp)</td>
<td></td>
</tr>
<tr>
<td>2745 (tcp)</td>
<td>Bagle variant</td>
<td>3127-3128 (tcp)</td>
<td>myDoom</td>
</tr>
<tr>
<td>3250 (tcp)</td>
<td>State Sync Protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* = can be opened upon valid business need request/scan

Distribution Firewall Configuration – Blocked Services
Distribution firewalls are used to provide authenticated and protected networking access in open areas and to protect specific business services which are remotely located. Network traffic sourced from the inside and return traffic is allowed; all traffic sourced from the outside is blocked.

Server Farm Firewall Configuration – Blocked Services
The server farm firewall is used to protect the campus main servers including mail servers, web servers, and database servers from the internet and other parts of the campus. Network traffic sourced from the inside and return traffic is allowed; all traffic sourced from the outside is blocked.

Firewall backups should be performed via an internally situated backup mechanism, e.g., tape drive. Firewall backups should not be written to any backup servers located on non-protected networks, as this may open a potential security hole to that network.

Logs
The firewall will be configured to use system logging (syslog) to export its log messages to designated syslog servers. The firewall logs will be backed up and archived in accordance with current practices implemented on the syslog server. The firewall will be configured to reject all SNMP requests. At a minimum, the firewall 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

Firewalls log activity, and firewall 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.

Firewall Physical Security
All Old Dominion University firewalls must be located in locked rooms accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management. The placement of firewalls in the open area within a general-purpose data processing center is prohibited; although placement within a separately locked rooms or areas within a general data processing center is acceptable.

Responsibilities
The Information Security Officer is responsible for ensuring the implementation of the requirements of the firewall standards. Daily operation and maintenance of the firewall 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 more trusted network may request via a FootPrints ticket (or email if Footprints is unavailable), a firewall “rule” 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 Information Security Officer (ISO) 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 firewall changes to stabilize a network infrastructure situation such as an attack or compromise can be made as required with written notification to the ISO seeking permanent changes if necessary after the fact.

Firewall configurations will be reviewed annually or when there are major changes to the network requirements that may warrant significant changes to the firewall. 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 firewall requests must come from the system owner. Please review the system owner list located in the ACL Request Procedures document.

To place a firewall 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 firewall rule modification request.
Have a business need that requires access campus resources from Internet?

Get authorization For request

Request approved by system owner?

yes

Private Server

Public or private server?

Public Server

A small group of employees

Vendor or contractors

Students with granted exception

many employees and students

large amount of students

entire internet community

Discuss with OCCS security Team about opening VPN or firewall ticket

VPN supported services

yes

Open vpn ticket

Limited source IP addresses allowed on border firewall

no

Discuss with OCCS security team about services needs to be opened

public or private server?

yes

get authorization

for request

request approved by system owner?

no

pass scan?

no

server admin receives scan report. OCCS security team finish firewall request

yes

server admin receives scan report. OCCS security team finish firewall request

public server?

yes

public server

no

private server

VPN supported services

open vpn ticket

limited source IP addresses allowed on border firewall

server admin receives scan report and fixes problem, then request another scan

Pass scan?

no