Data Center Firewall Customer Guide

Introduction

This guide is an introduction to how the Office of Information Technology is implementing firewall services in the data center. This guide is supplemental to any general documentation on firewalls or documentation provided by vendors for specific firewall hardware.

The new data center firewall service marks a significant change to how system access is controlled, audited and monitored. With this change, however, OIT will require more specific information on how end-users access systems in the data center, how administrators access their systems and how systems interact with other systems inside and outside the data center. As a result, the OIT data center firewall service now requires that administrators define connections coming into (inbound access) and out of (outbound access) the data center.

Inbound Access

This access category covers connections initiated by end-users, administrators or other systems (source) to a system or application hosted in the data center (destination). These are new connections coming from customers to the application or system in the data center.

When specifying the source for a particular connection, administrators will choose from the groups below. When specifying the destination, administrators will need to provide the IP and port.

- **VPN**
  - Connections from a predefined network range associated with the vpn user.
- **Server Administrator Network**
  - Connections from a defined network used by the server or
application administrators.

- **Campus**
  - Connections from any UNLV network.
- **Internet**
  - Connections from anywhere.

The following example illustrates how we would define a rule to allow connections to http://app.unlv.edu.

```
All UNLV campus networks –new connection  IP 192.168.0.10, TCP Port 80
```

**Outbound Access**

This access category covers new connections initiated by system or application in the data center (source) to an application or system outside the datacenter (destination). These are new connections leaving systems in the data center to systems outside the data center firewall.

```
When specifying the source for a particular connection, administrators
will provide an IP address or a subnet. When specifying the destination, administrators will need to provide a specific IP address and port. The example below shows how we would define a connection from our servers in the datacenter to an FTP server outside the data center firewall.

The outbound access source, in this case all the servers, is represented as the subnet 192.168.0.0/24 and the destination address is 74.125.239.6. FTP relies on port 21. Given this information the firewall rule is defined as:

192.168.0.0 –new connection IP 74.125.239.6, TCP Port 21

**Web Proxy Connections**

This access category covers new connections initiated by an administrator or system (source) to a web site (destination) that is commonly used by a group of servers. These are new connections created for common purposes such as server OS updates.

When specifying the source for a particular connection, administrators will provide an IP address or a subnet. When specifying the destination, administrators will need to provide a URL as the destination. The example below
shows how typical connections to Microsoft Update would be defined.

The outbound access source, in this case all the servers, is represented as the subnet 192.168.0.0/24 and the destination is update.microsoft.com. The destination is added to the list of allowed destinations for the web proxy and all MS servers are allowed to request updates from update.microsoft.com.

**Intra-Data Center Access**

This type of access represents a common situation for systems in the data center. One system might need to communicate with another system, both of which are located in the data center but do not share the same network subnet. An example of this is an application server on one subnet that needs to communicate with a database server on another subnet. In this case, the standard will be to allow all traffic from any data center network to reach the destination IP and port. If required, rules can be more granular to allow only point-to-point connections.

Quick link: http://goo.gl/EGxM1