OCF internet/networking border

(and how to access OCF from outside)
internet (IST)

example setup
(if we didn't have a firewall)
internet

cisco firewall (owned by IST)

ethernet jack in our server room
black cable (no firewall)

orange cable (yes firewall)

(not actually plugged in to anything)
ok, everything is behind firewall… what does that look like?
## Configuration > Firewall > Access Rules

### inside 169.229.10.0 (3 incoming rules)

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
<th>Logging</th>
<th>Time</th>
<th>Descr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>smtp-outbound</td>
<td>any</td>
<td>smtp</td>
<td>Per...</td>
<td>19866</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✔️</td>
<td>any</td>
<td>any</td>
<td>smtp</td>
<td>Deny</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✔️</td>
<td>ocf-hearst</td>
<td>any</td>
<td>ip</td>
<td>Per...</td>
<td>1153</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### outside 169.229.10.0 (16 incoming rules)

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>any</td>
<td>ocf-hearst</td>
<td>icmp</td>
<td>Per...</td>
<td>6078</td>
</tr>
<tr>
<td>2</td>
<td>✔️</td>
<td>any</td>
<td>web</td>
<td>http</td>
<td>Per...</td>
<td>1130</td>
</tr>
<tr>
<td>3</td>
<td>✔️</td>
<td>any</td>
<td>login</td>
<td>ssh</td>
<td>Per...</td>
<td>7989</td>
</tr>
<tr>
<td>4</td>
<td>✔️</td>
<td>any</td>
<td>kerberos</td>
<td>kerberos5</td>
<td>Per...</td>
<td>167</td>
</tr>
<tr>
<td>5</td>
<td>✔️</td>
<td>any</td>
<td>ldap</td>
<td>ldaps</td>
<td>Per...</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>✔️</td>
<td>any</td>
<td>ns</td>
<td>domain</td>
<td>Per...</td>
<td>1180</td>
</tr>
<tr>
<td>7</td>
<td>✔️</td>
<td>ocf-hearst</td>
<td>puppet</td>
<td>puppetm...</td>
<td>Per...</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>✔️</td>
<td>sns</td>
<td>ocf-hearst</td>
<td>ip</td>
<td>Per...</td>
<td>4868</td>
</tr>
<tr>
<td>9</td>
<td>✔️</td>
<td>any</td>
<td>flood</td>
<td>ip</td>
<td>Per...</td>
<td>1629</td>
</tr>
<tr>
<td>10</td>
<td>✔️</td>
<td>any</td>
<td>hozer</td>
<td>ip</td>
<td>Per...</td>
<td>1435</td>
</tr>
<tr>
<td>11</td>
<td>✔️</td>
<td>any</td>
<td>fallingrocks</td>
<td>rsync</td>
<td>Per...</td>
<td>6313</td>
</tr>
<tr>
<td>12</td>
<td>✔️</td>
<td>any</td>
<td>ocf-hearst</td>
<td>ftp-passive</td>
<td>Per...</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>✔️</td>
<td>sns</td>
<td>ocf-hearst</td>
<td>ip</td>
<td>Per...</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>✔️</td>
<td>any</td>
<td>smtp-inbound</td>
<td>smtp</td>
<td>Per...</td>
<td>1413</td>
</tr>
<tr>
<td>15</td>
<td>✔️</td>
<td>any</td>
<td>supernova</td>
<td>domain</td>
<td>Per...</td>
<td>190</td>
</tr>
<tr>
<td>16</td>
<td>✔️</td>
<td>mercury</td>
<td>pollution</td>
<td>https</td>
<td>Per...</td>
<td>232</td>
</tr>
</tbody>
</table>

### Global (1 implicit rule)

<table>
<thead>
<tr>
<th>#</th>
<th>Enabled</th>
<th>Source Criteria:</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Hits</th>
<th>Logging</th>
<th>Time</th>
<th>Descr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>any</td>
<td>any</td>
<td>ip</td>
<td>Deny</td>
<td></td>
<td></td>
<td></td>
<td>Implicit rule</td>
</tr>
</tbody>
</table>

Access Rule Type  IPv4 and IPv6  IPv4 Only  IPv6 Only
internet

all outbound traffic allowed*

*one exception: email (for spam reasons)

desktops (computer lab)

services (web, email, ...)

login (ssh)
internet

no inbound allowed

desktops (computer lab)
services (web, email, ...)
login (ssh)
internet

- some inbound allowed

- deskt ops (computer lab)
- services (web, email, ...)
- login (ssh)
internet

- desktopen (computer lab)
- services (web, email, ...)
- login (ssh)

some inbound allowed (ssh)
what if I want to access a desktop or server remotely?

- desktops (computer lab)
- services (web, email, ...)
- login (ssh)

X
what if I want to access a desktop or server remotely?

bastions!

desktops (computer lab)

services (web, email, ...)

login (ssh)
first, connect via SSH to a login server
internet

**bastions!**
first, connect via SSH to a login server
then, connect to anything else

desktops
(computer lab)

login
(ssh)
OCF has two login servers:

tsunami
public, all OCF users can access it
32 GB RAM, 16 VCPUs (lives on hal)
OCF has two login servers:

**tsunami**
public, all OCF users can access it
32 GB RAM, 16 VCPUs (lives on hal)

**supernova**
private, only OCF staff can access it
8 GB RAM, 16 VCPUs (lives on hal)
OCF has two login servers:

**tsunami**
public, all OCF users can access it
32 GB RAM, 16 VCPUs (lives on hal)
restricted access to other OCF stuff

**supernova**
private, only OCF staff can access it
8 GB RAM, 16 VCPUs (lives on hal)
full access to other OCF stuff
always connect to supernova first!

0. start on my computer

```
ckuehl@neon:~$ ssh ckuehl@supernova.ocf.berkeley.edu
Linux supernova 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64
Last login: Mon Sep 22 16:11:08 2014 from neon.techxonline.net
ckuehl@supernova:~$ ssh firestorm
ckuehl@firestorm:~$ ssh firestorm's password:
Linux firestorm 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64
Last login: Thu Aug 28 18:48:07 2014 from supernova.ocf.berkeley.edu
Could not chdir to home directory /home/c/ck/ckuehl: No such file or directory
ckuehl@firestorm:/$
```
always connect to supernova first!

0. start on my computer
1. connect to supernova
always connect to supernova first!

0. start on my computer
   + ssh ckuehl@supernova.ocf.berkeley.edu
   + ssh firestorm

1. connect to supernova
   + $ ssh ckuehl@supernova.ocf.berkeley.edu
   + $ ssh firestorm
   + Could not chdir to home directory /home/c/ck/ckuehl: No such file or directory

2. connect to actual destination (in this example, firestorm)
one thing we skipped...
internet

- desktops (computer lab)
- services (web, email, ...)
- login (ssh)

hozers (your staff VMs!)
internet

X

desktops (computer lab)

services (web, email, ...)

login (ssh)

hozers (your staff VMs!)

LET THROUGH
ALL THE TRAFFIC
congrats!
now you can log in to the OCF!