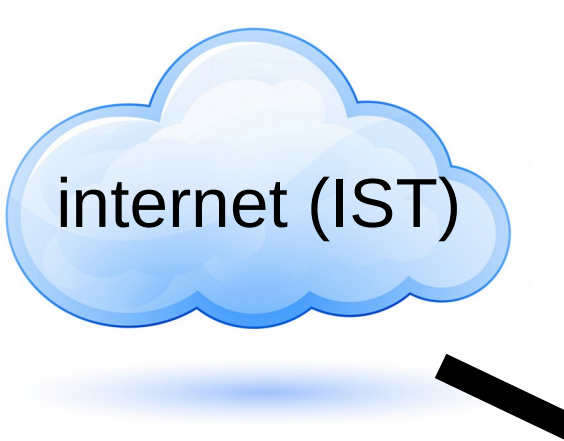
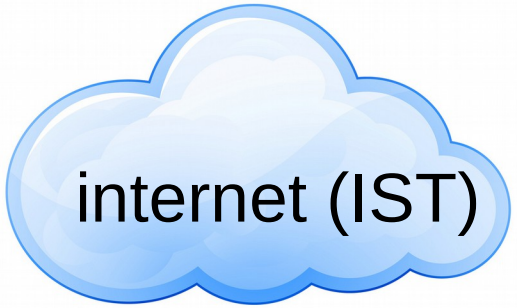
OCF internet/networking border

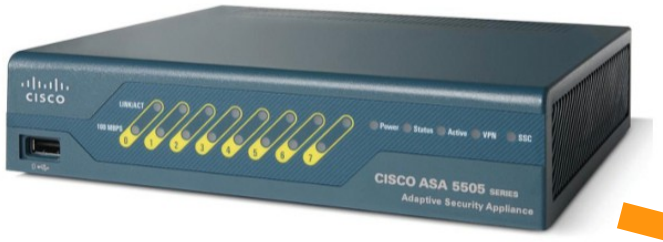
(and how to access OCF from outside)



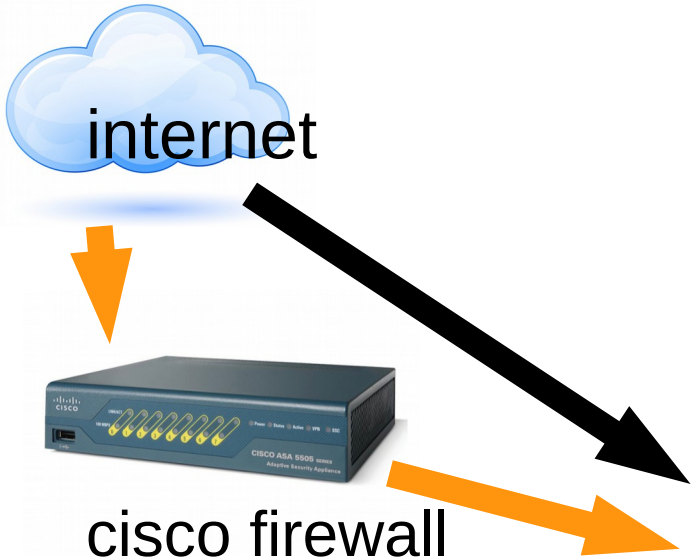
example setup
(if we didn't have a firewall)

actual setup





cisco firewall
(owned by IST)



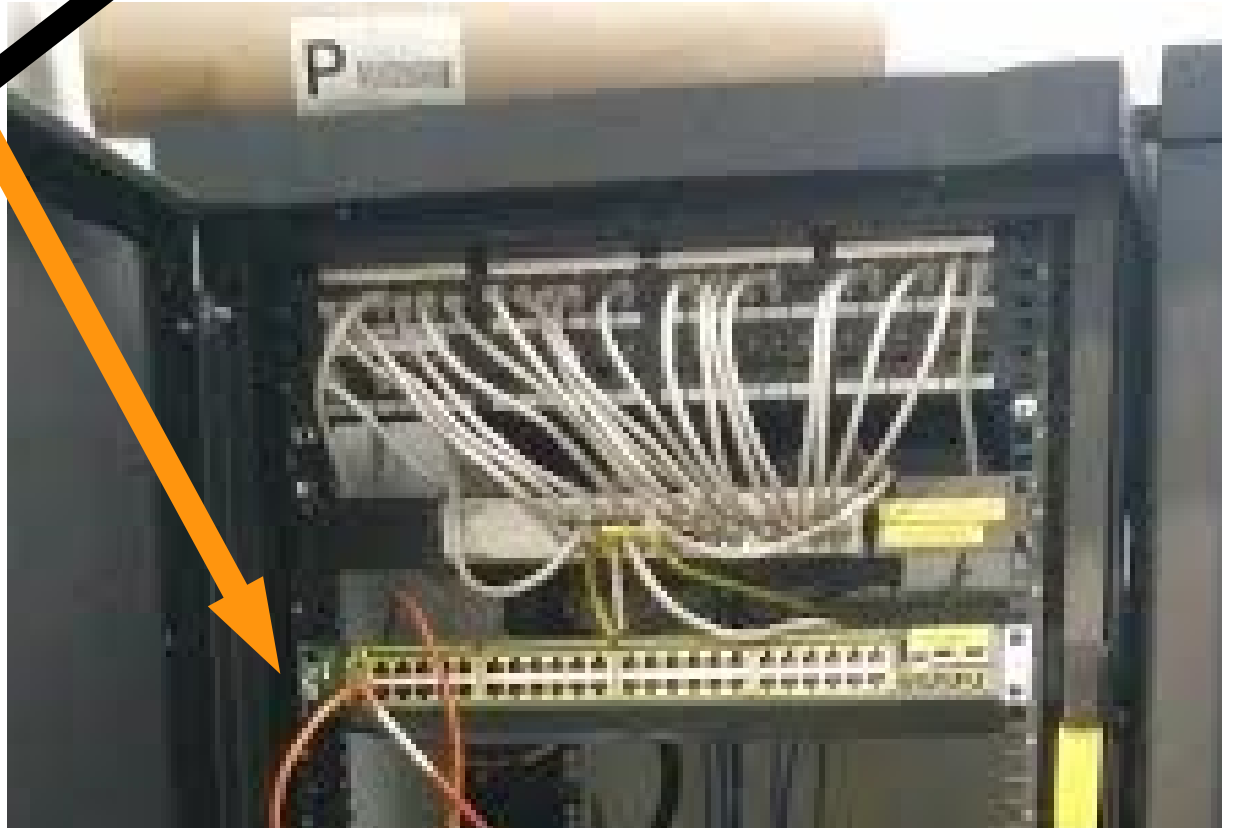
ethernet jack in our server room

black cable
(no firewall)

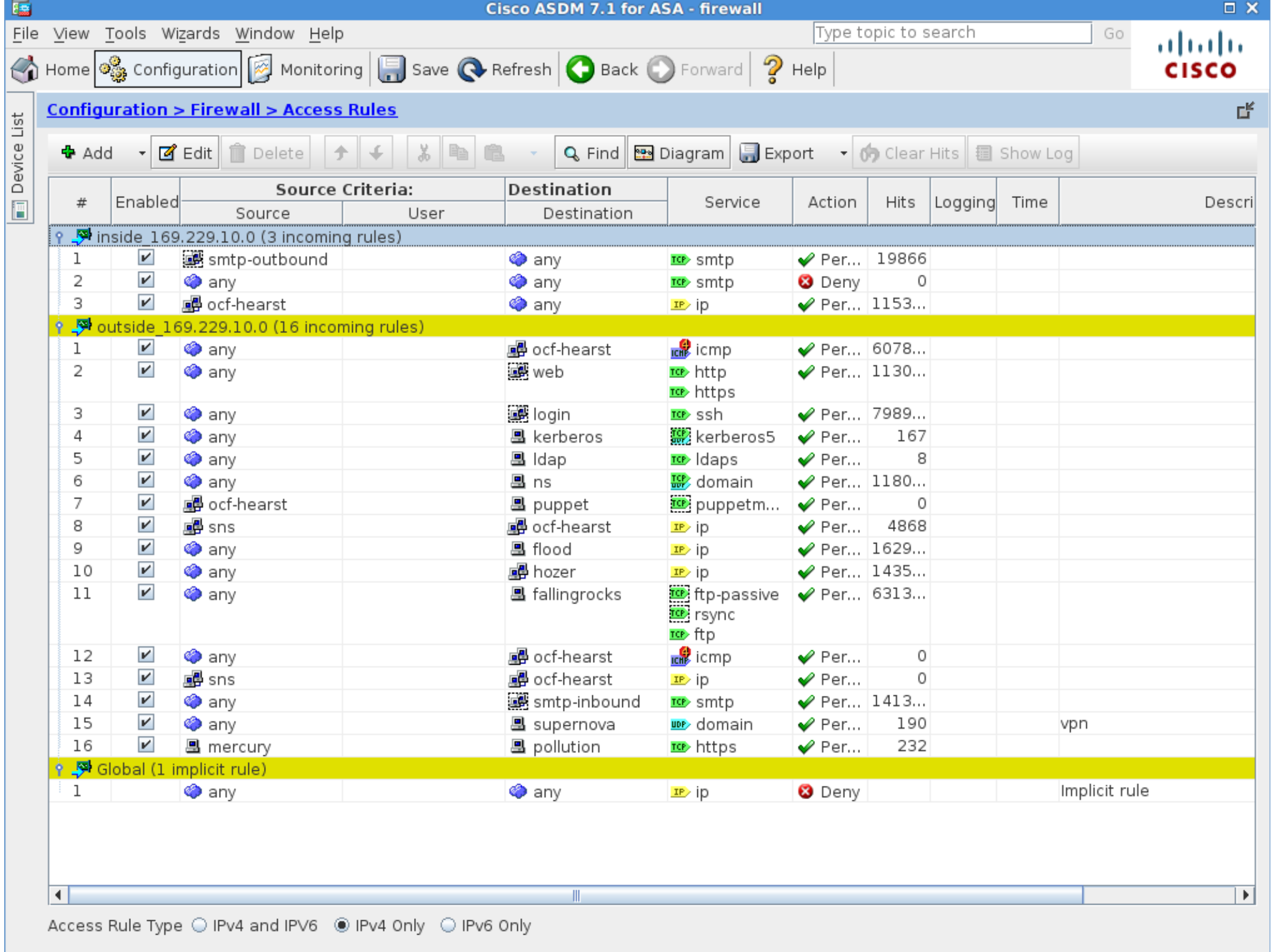
X

(not actually
plugged in to
anything)

orange cable
(yes firewall)



ok, everything is behind firewall... what does that look like?


Cisco ASDM 7.1 for ASA - firewall
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Clear Hits Show Log
Enabled Source Criteria: Source User Destination: Destination Service Action Hits Logging Time Descri
inside_169.229.10.0 (3 incoming rules)
1 smtp-outbound any smtp Per... 19866
2 any any smtp Deny 0
3 ocf-hearst any ip Per... 1153...
outside_169.229.10.0 (16 incoming rules)
1 any ocf-hearst icmp Per... 6078...
2 any web http https Per... 1130...
3 any login ssh Per... 7989...
4 any kerberos kerberos5 Per... 167
5 any ldap ldaps Per... 8
6 any ns domain Per... 1180...
7 ocf-hearst puppet puppetm... Per... 0
8 sns ocf-hearst ip Per... 4868
9 any flood ip Per... 1629...
10 any hozer ip Per... 1435...
11 any fallingrocks ftp-passive rsync ftp Per... 6313...
12 any ocf-hearst icmp Per... 0
13 sns ocf-hearst ip Per... 0
14 any smtp-inbound smtp Per... 1413...
15 any supernova domain Per... 190 vpn
16 mercury pollution https Per... 232
Global (1 implicit rule)
1 any any ip Deny Implicit rule
Access Rule Type IPv4 and IPV6 IPv4 Only IPv6 Only

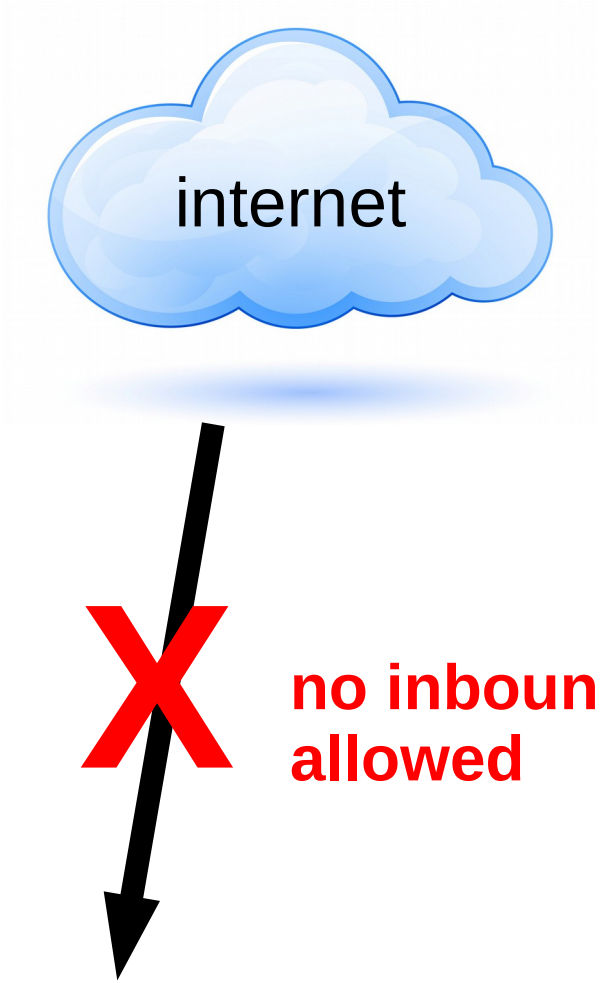
all outbound traffic allowed*

***one exception: email (for spam reasons)**

desktops (computer lab)

services (web, email, ...)

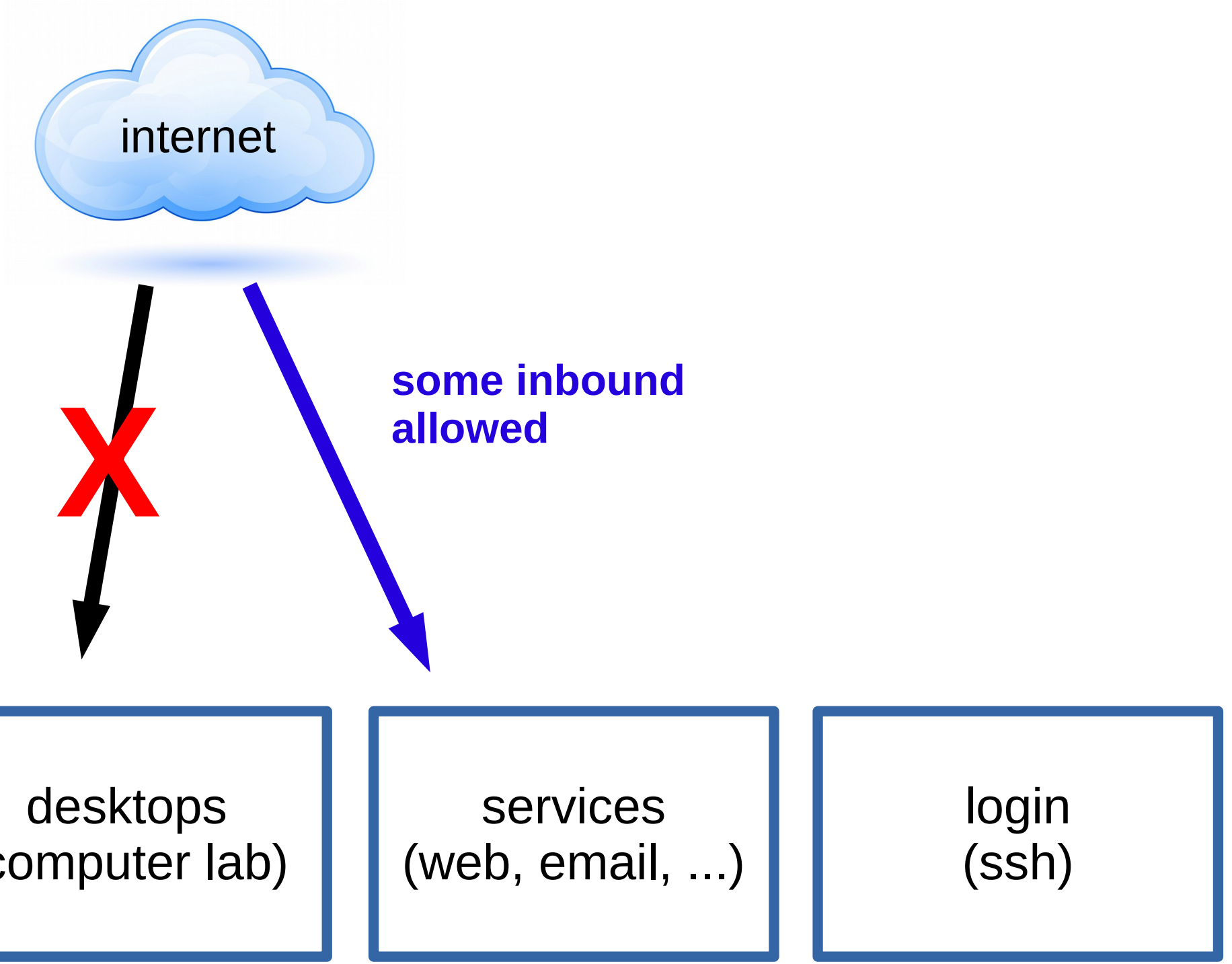
login (ssh)

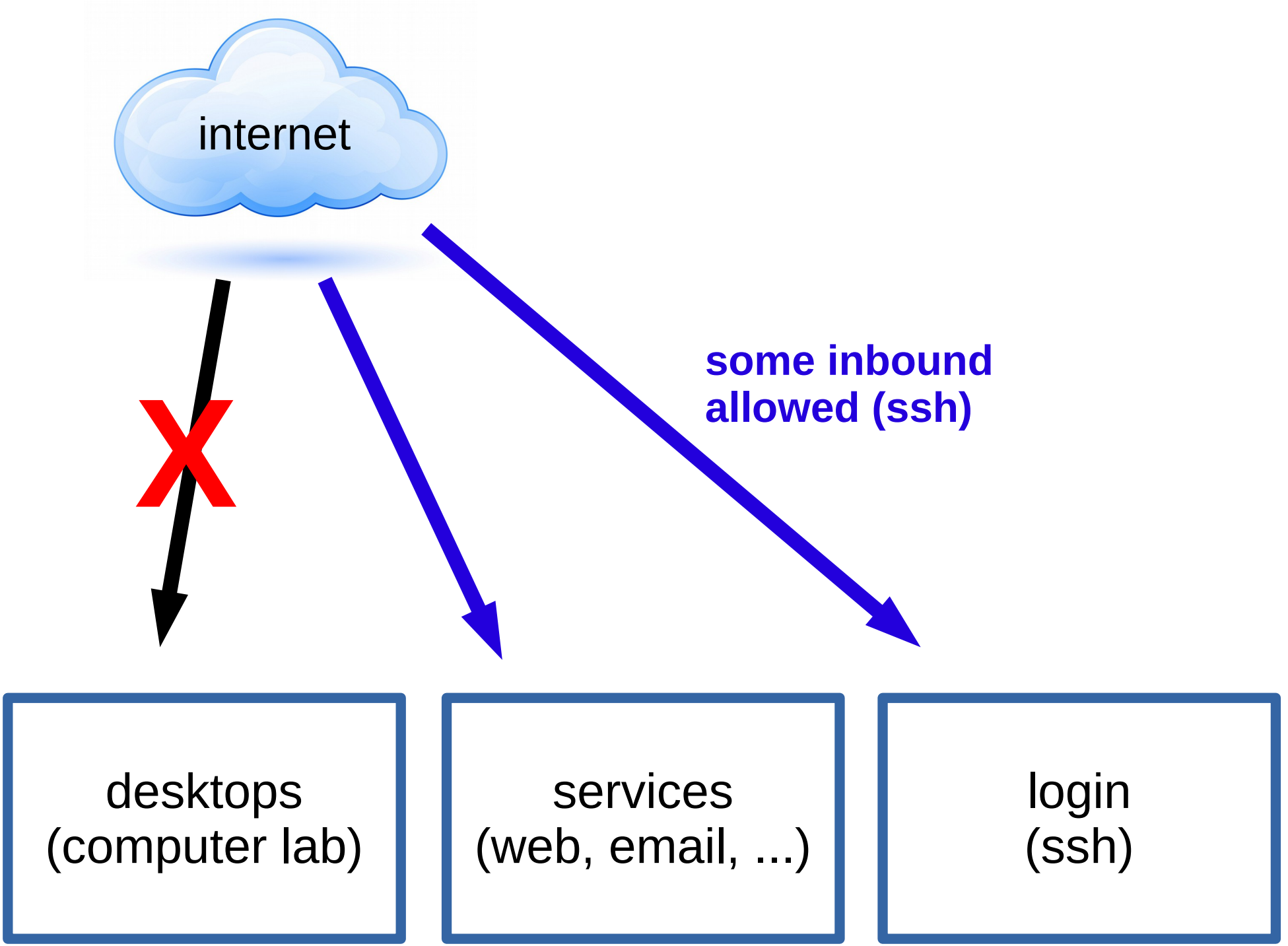


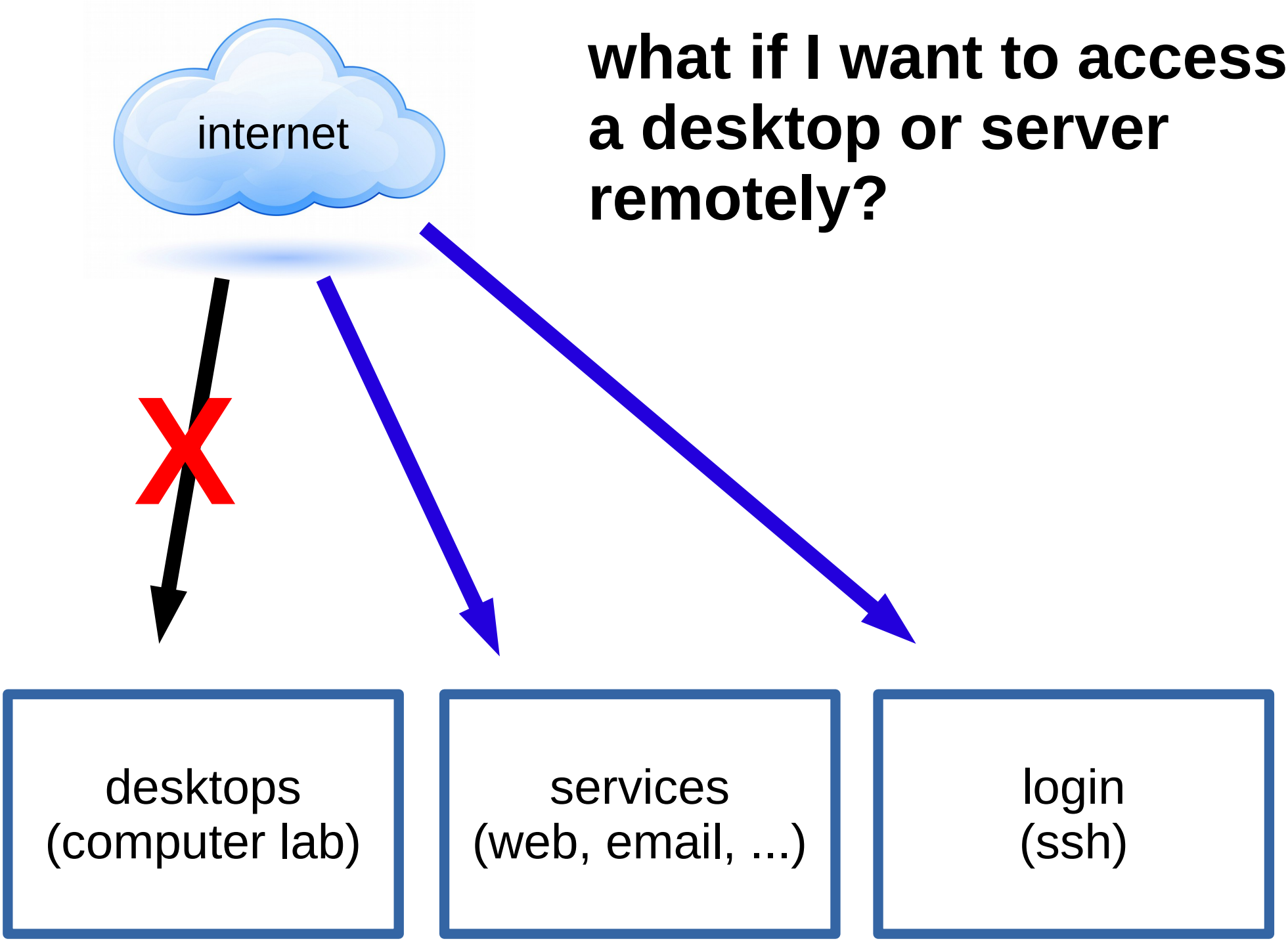
desktops
(computer lab)

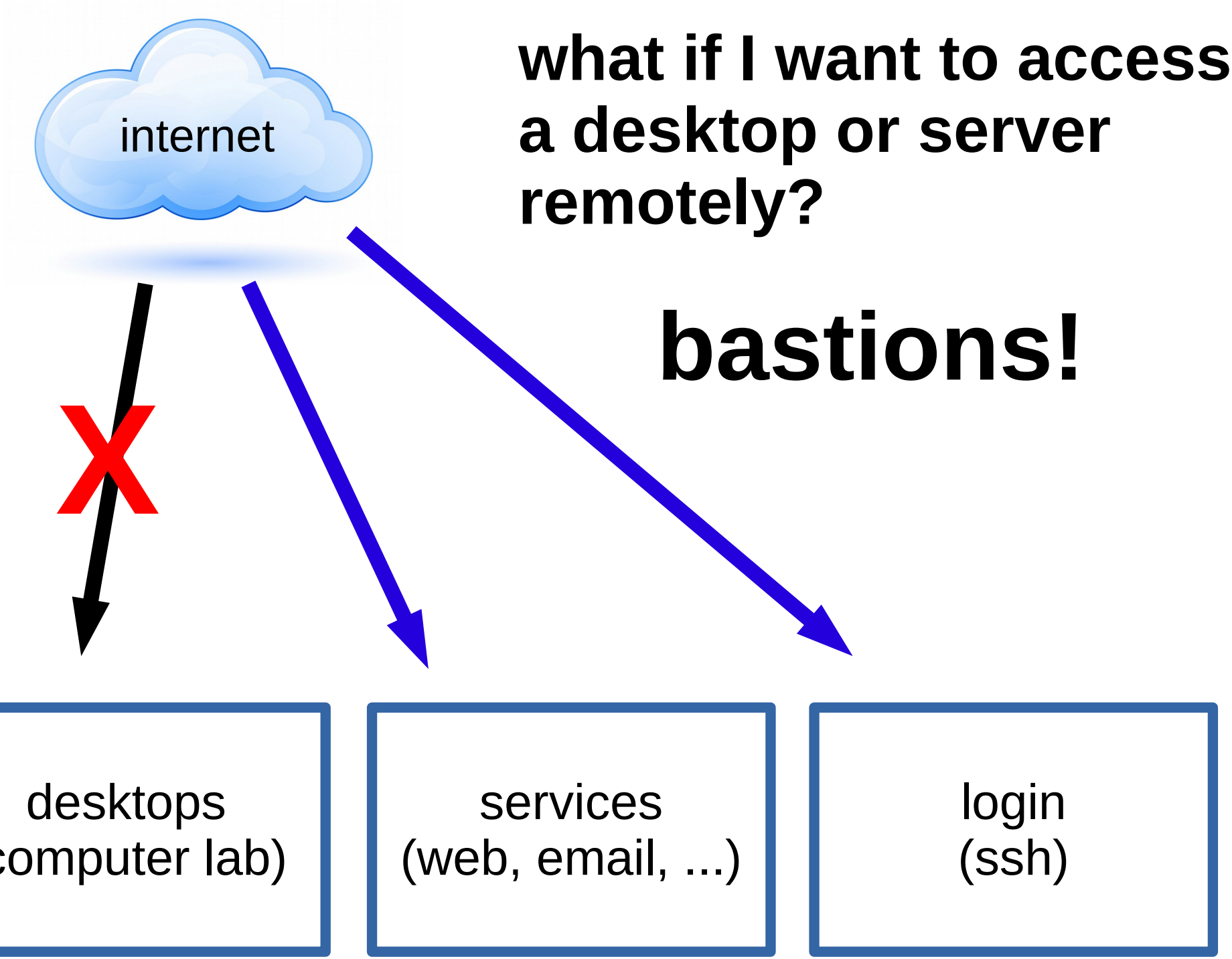
services
(web, email, ...)

login
(ssh)


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


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


internet
what if I want to access a desktop or server remotely?
desktops (computer lab)
services (web, email, ...)
login (ssh)


internet
what if I want to access a desktop or server remotely?
bastions!
desktops (computer lab)
services (web, email, ...)
login (ssh)

bastions!

first, connect via SSH to a login server

desktops
(computer lab)

login
(ssh)

bastions!

first, connect via SSH to a login server

then, connect to anything else

desktops (computer lab)

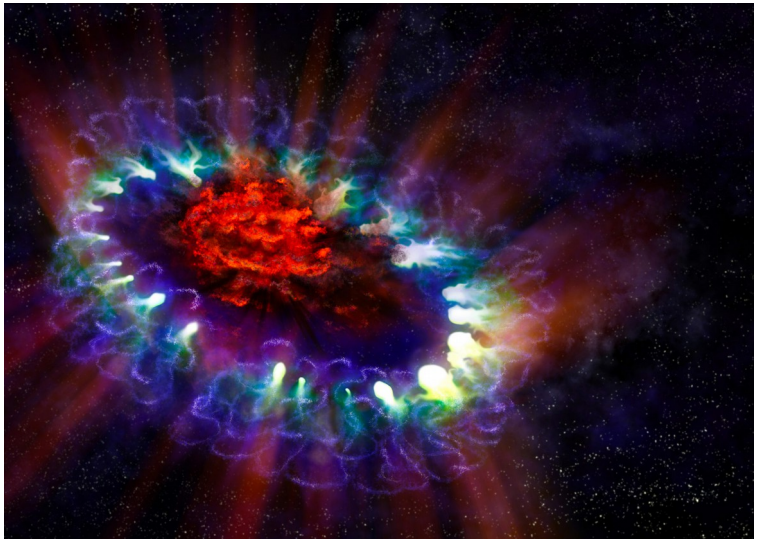
login (ssh)

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:

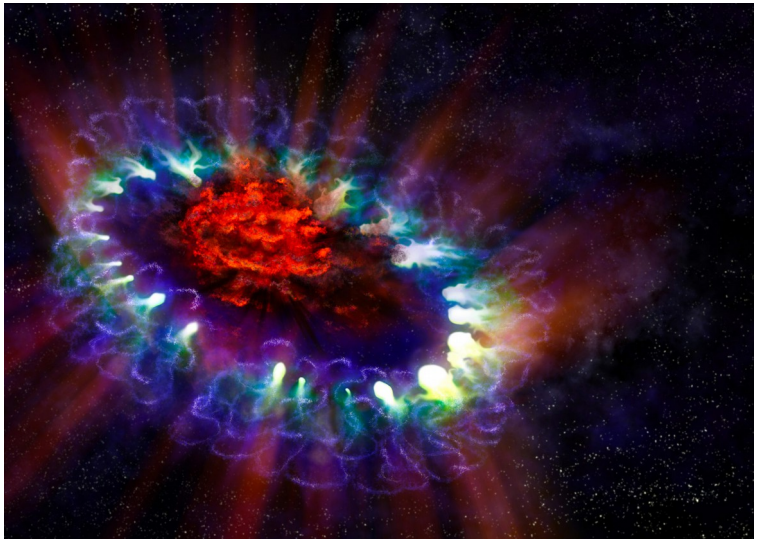
tsunami
public, all OCF users can access it
32 GB RAM, 16 VCPUs (lives on hal)



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!

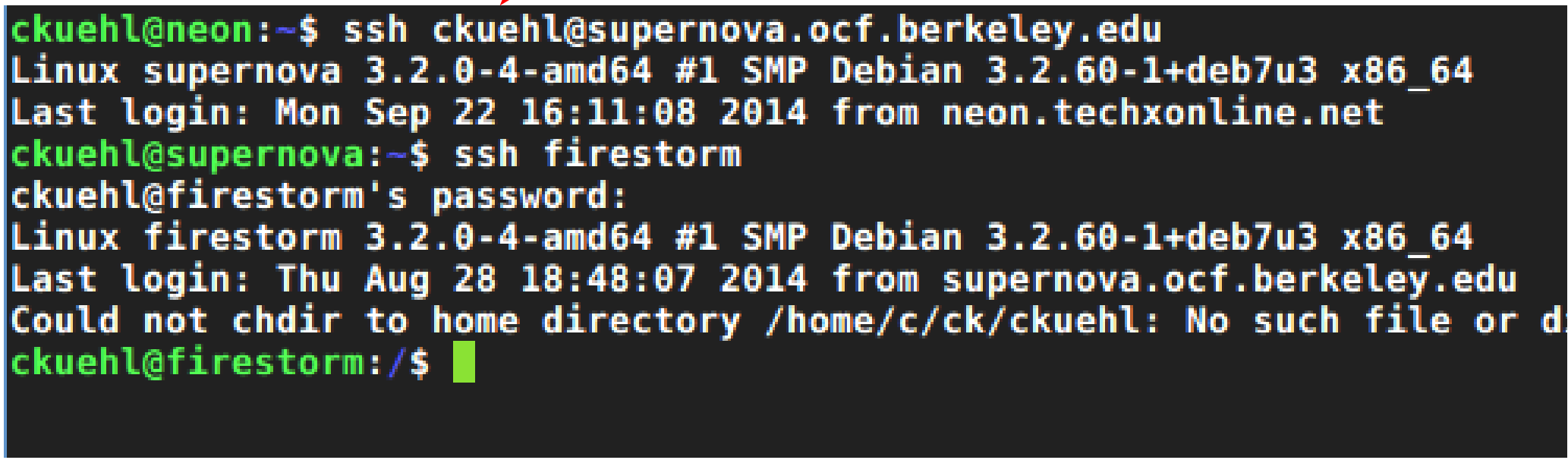
0. start on my computer

```
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'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 d
ckuehl@firestorm:/$
```

always connect to supernova first!

0. start on my computer

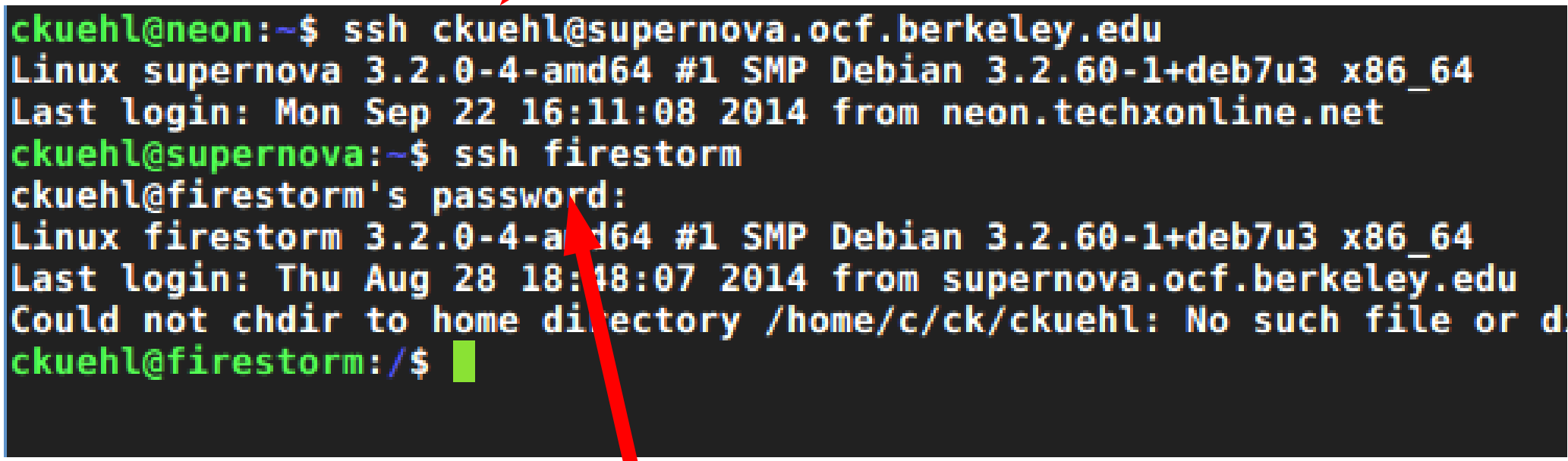
1. connect to supernova



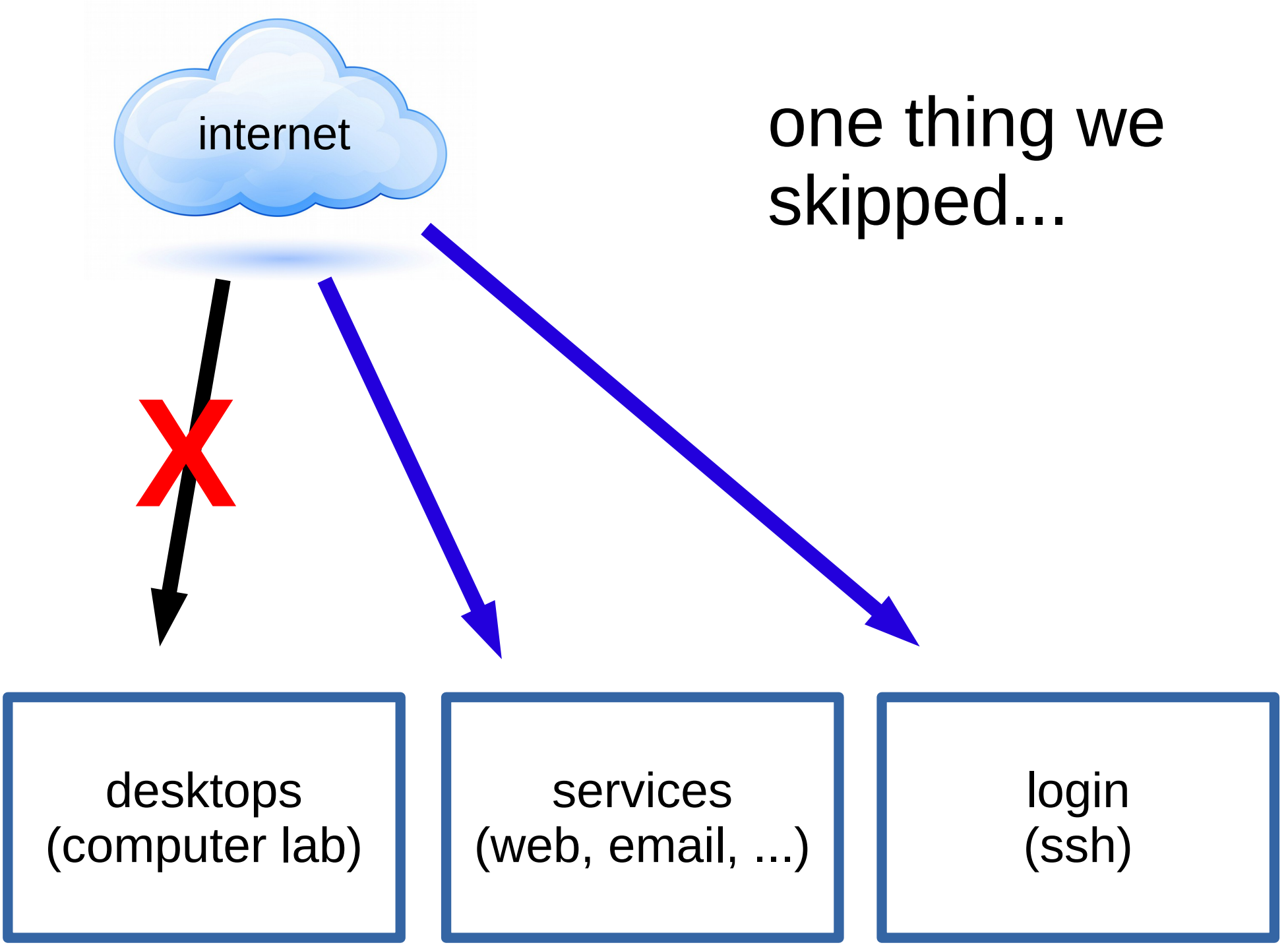
always connect to supernova first!

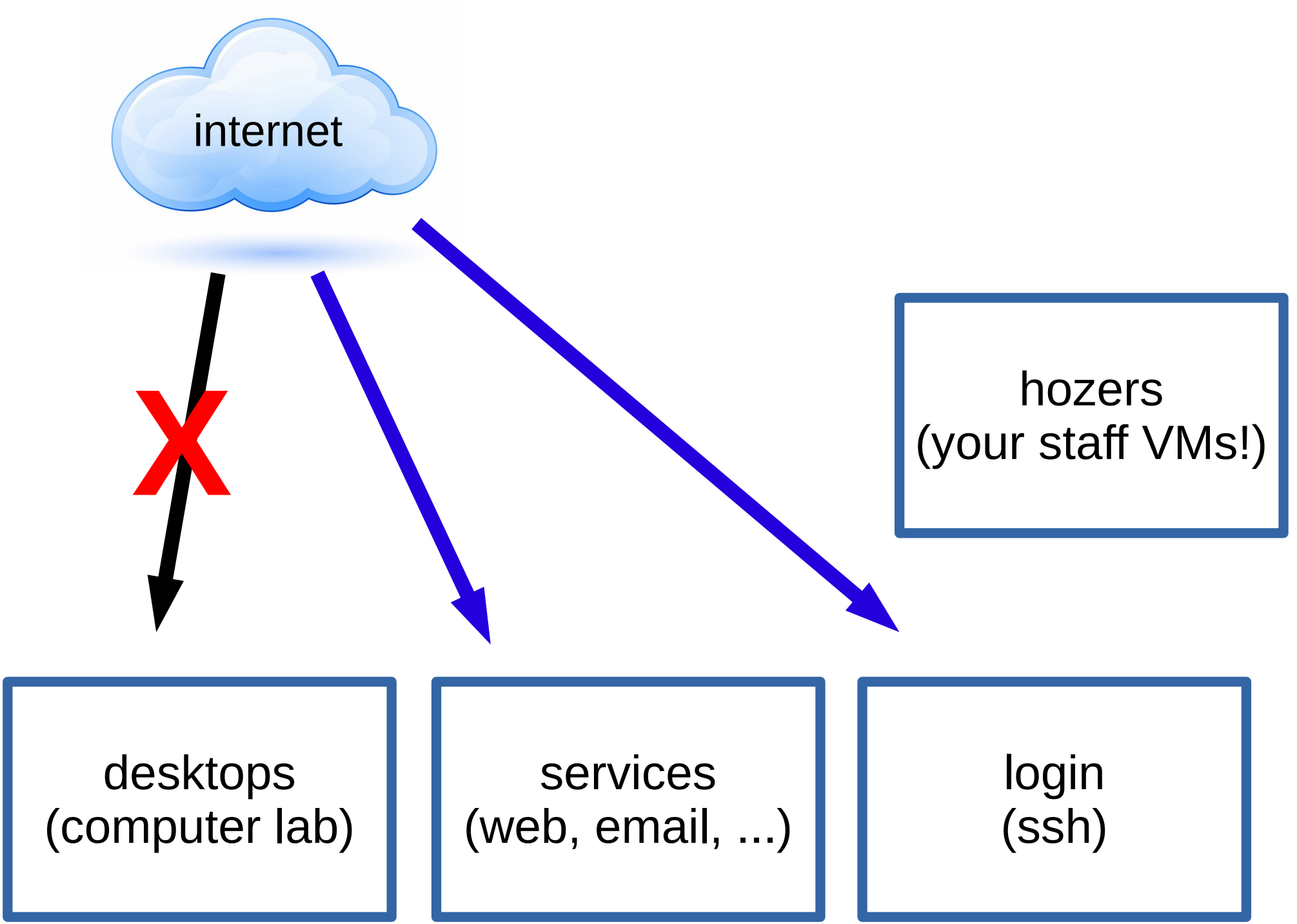
0. start on my computer

1. connect to supernova



2. connect to actual destination (in this example, firestorm)


internet
one thing we skipped...
desktops (computer lab)
services (web, email, ...)
login (ssh)


internet
hozers
(your staff VMs!)
desktops
(computer lab)
services
(web, email, ...)
login
(ssh)

hozers
(your staff VMs!)

desktops
(computer lab)

services
(web, email, ...)

login
(ssh)

congrats!

now you can log in to the OCF!