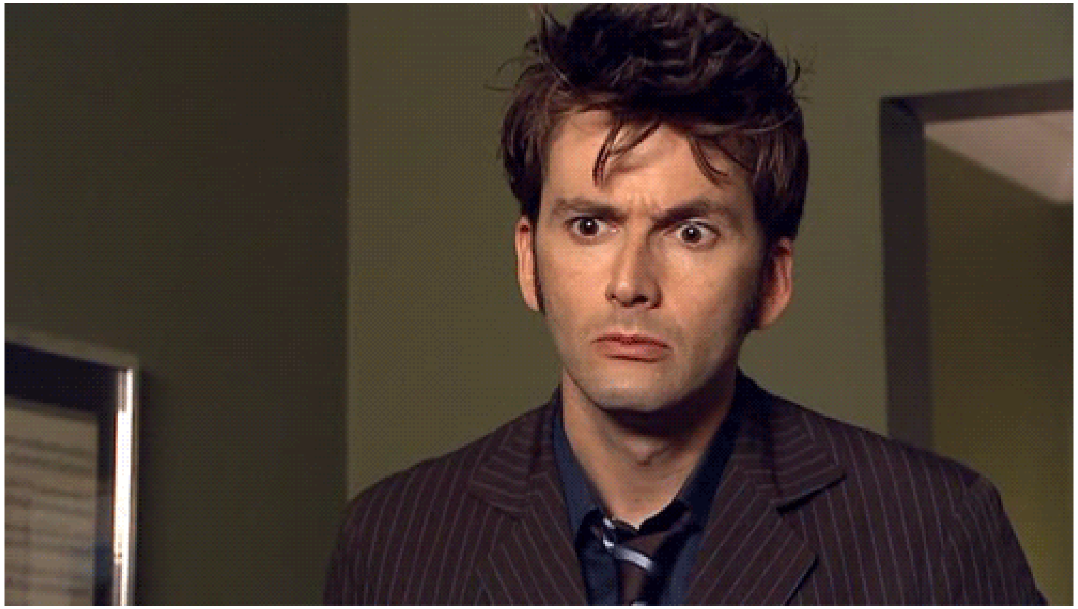
The firewall also gazes into you

About me

- @iangreenleaf
- Rails developer (backend, *not* devops)
- Hire me! dev@iangreenleaf.com

"What's the use of firewalls?"



Wide-open ports

Isn't that a little 1997?

Well…

MongoDB

- Local connections only by default
- Authentication possible, off by default

Sphinx full-text search

- Local connections possible, off by default
- No authentication

Memcached

- Local connections possible, off by default
- Authentication sorta possible, off by default

Redis

- Local connections possible, off by default
- Authentication possible, off by default
- Redis is open to the world by default
- It too offers weak authentication

Yikes

You *could* fix each of these individually

My ops policy:

Assume I am stupid

Default to the
least bad thing

Firewalls are dead
Long live firewalls

When you hear "firewall", do you think of...

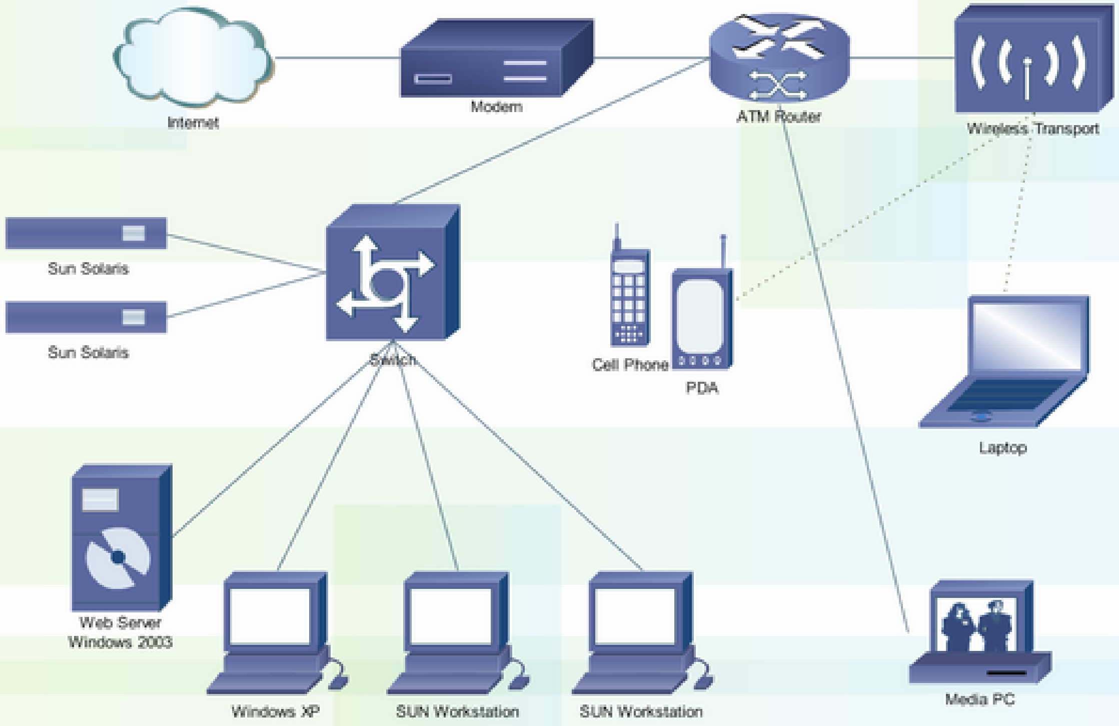
Network administrators

NATs

```
ssh me@server -p 2525
```

Keep it secret; keep it safe

Cisio Network Diagram



Stupid crap interfering with my ability to play World of Warcraft

Let go of your fear

Firewalls that don't suck

- Default to DENY
- Assume every machine is public
- Simple firewall on each machine

PSA: Make sure to open your SSH port!

iptables

ufw

Chef/Ansible

Because you *are* automating, right?

Chef

`firewall` cookbook

Chef

```
firewall 'ufw' do
  action :enable
end
```

Chef

```
firewall_rule 'default' do
  action :deny
end
```

Chef

```
firewall_rule 'ssh' do
  port     22
  action   :allow
end
```

Chef

```
firewall_rule 'http' do
  port     80
  protocol :tcp
  action   :allow
end
```

That wasn't so bad

Ansible

`ufw` module in 1.6+

Ansible

```
name: install ufw
apt: pkg=ufw state=present
```

Ansible

```
name: enable firewall
ufw: state=enabled policy=deny
```

Ansible

```
name: pass HTTP through firewall
ufw: rule=allow port=80 proto=tcp
```

Ansible

```
name: pass SSH through firewall
ufw: rule=allow name=OpenSSH
```

Extra credit: rate limiting

Rate limiting

```
name: pass SSH through firewall
ufw: rule=limit name=OpenSSH
```

That's it!

Fin