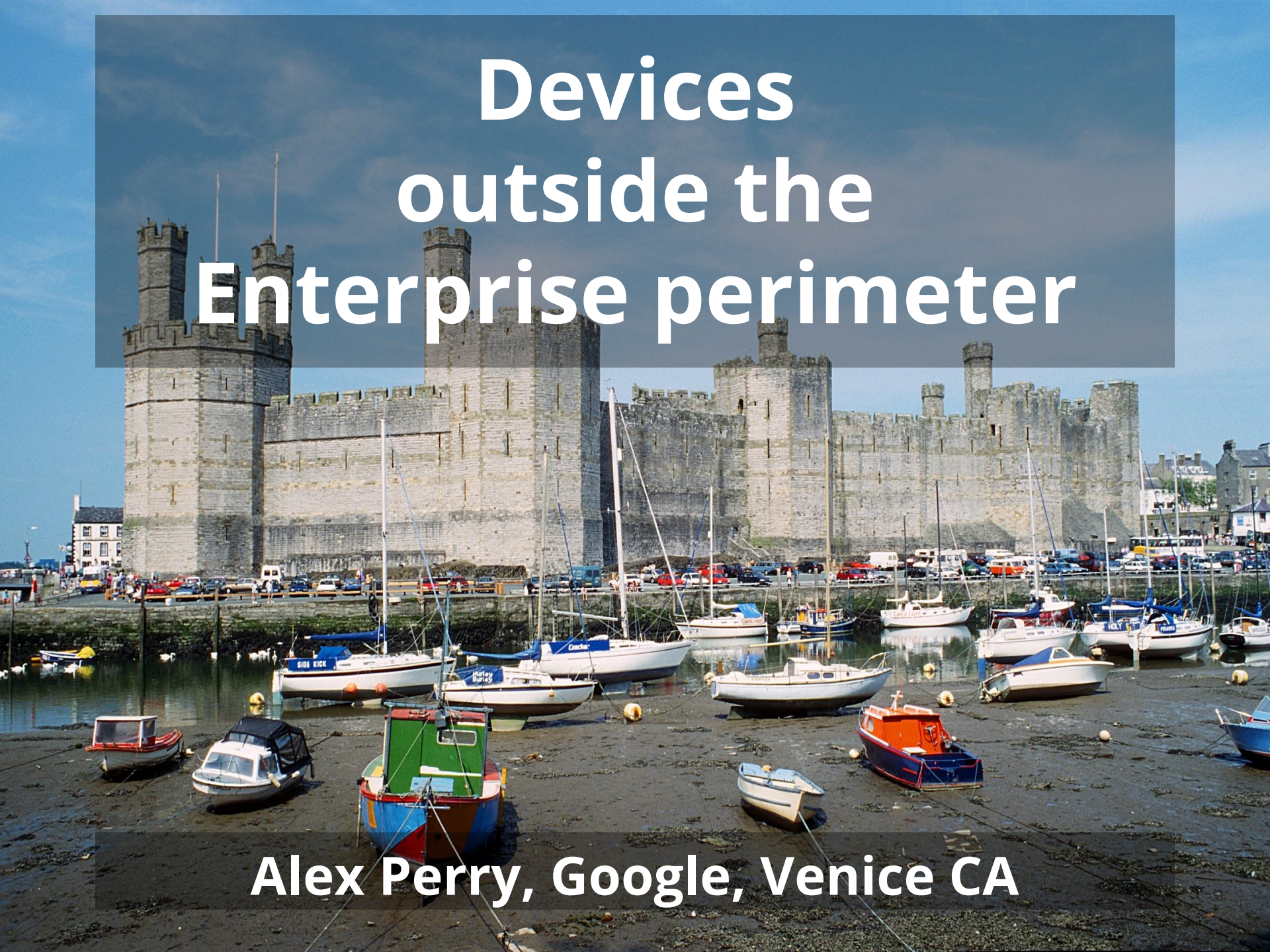


Devices outside the Enterprise perimeter

Alex Perry, Google, Venice CA

Outline

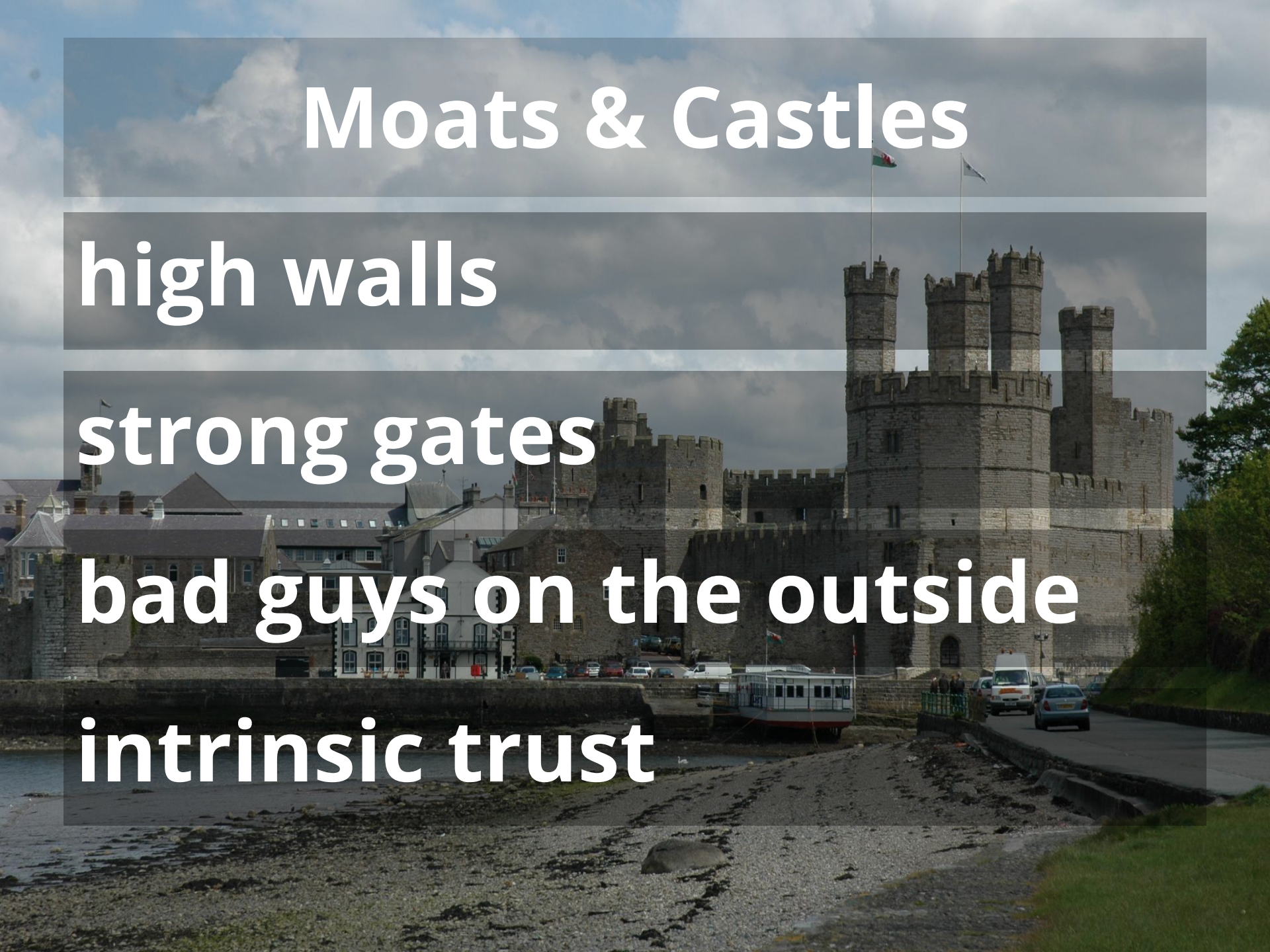
- Device diversity among users
- Many services and perimeters
- Usage across many perimeters
- The *Beyond Corp* architecture
- Administration / risk model
- Challenges and complications
- Directions and further work

Vision: User Experience

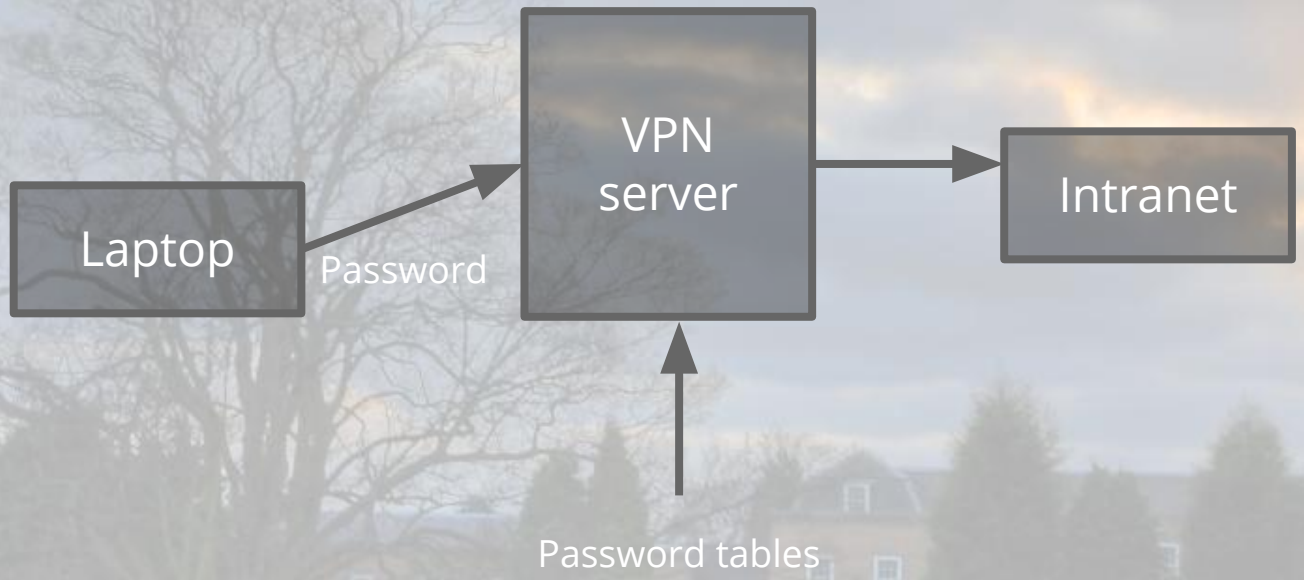
work from anywhere

cloud based workflows

limit access by policy only

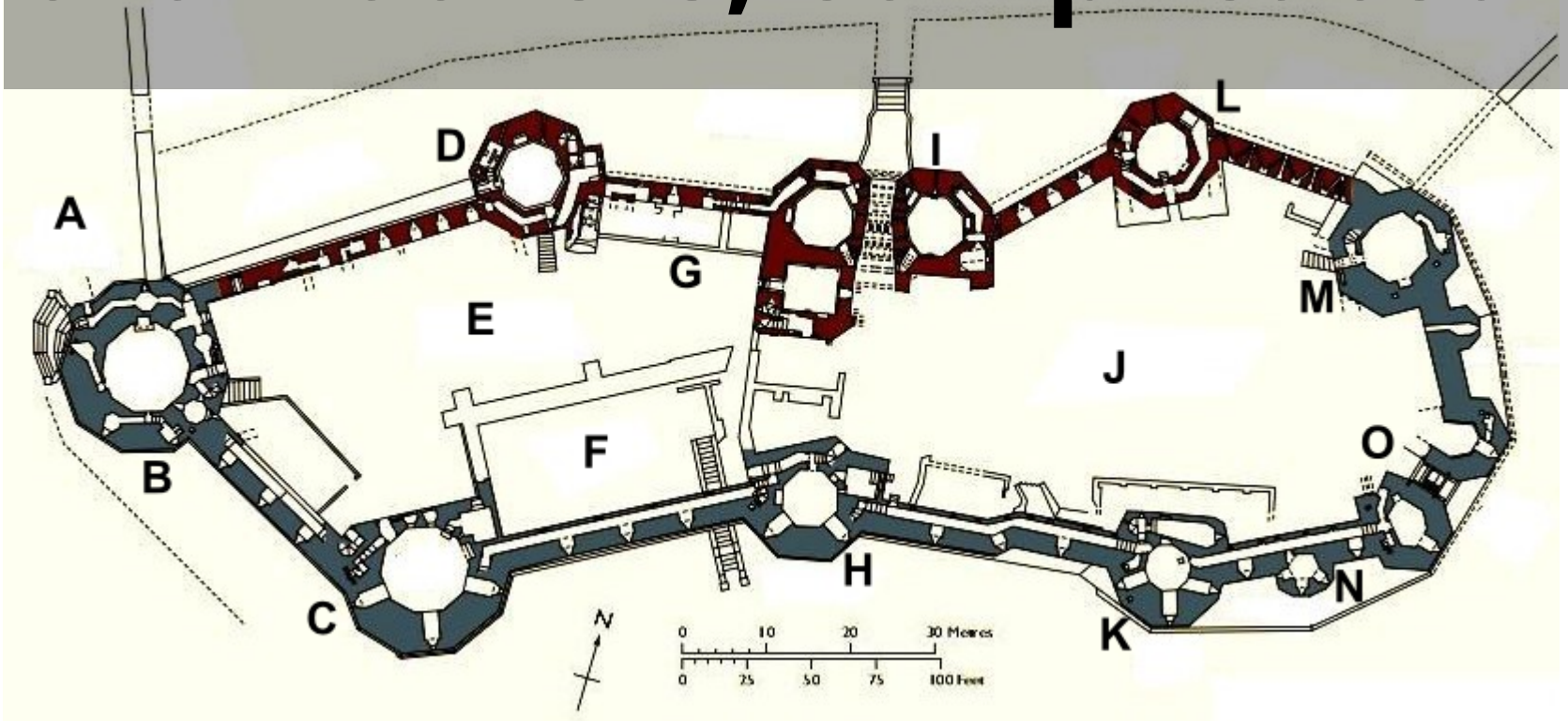

Moats & Castles
high walls
strong gates
bad guys on the outside
intrinsic trust

Usual Architecture

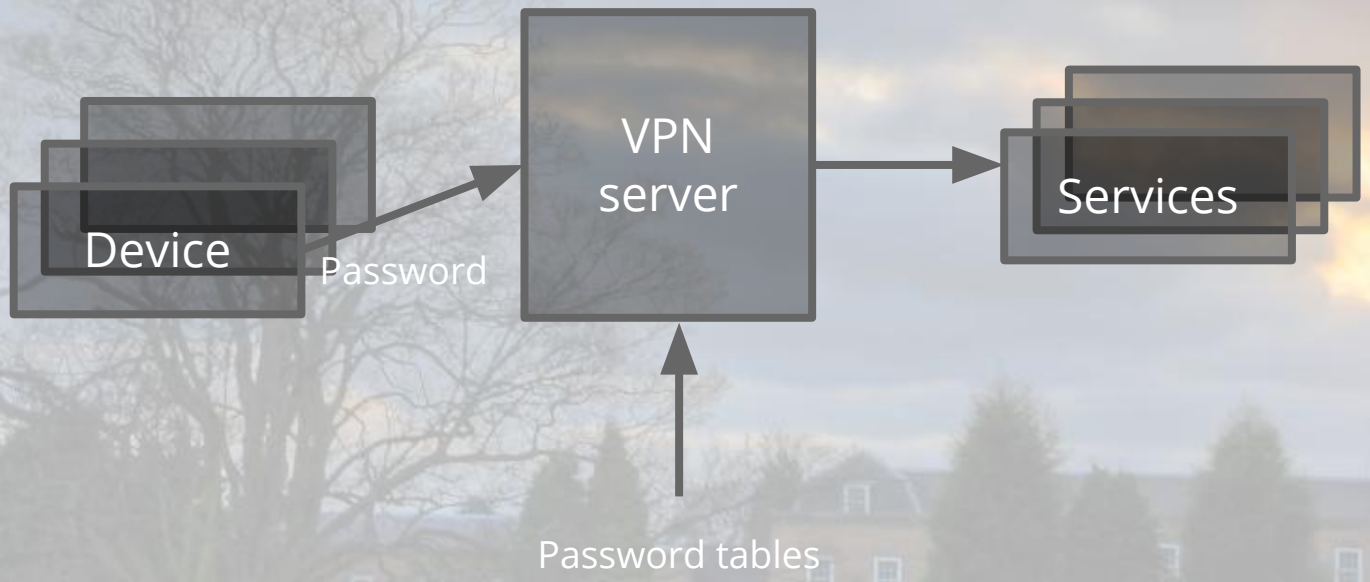


Devices not equivalent

Some are trusted more than others; complicated



Trying to fix architecture



One VPN configuration per service and per device type?
But then … how to use more than one at a time?


evolved attackers/attacks
hitting the weakest link
infect users when outside
user can pass firewall


Access SRE ...
No "Perimeter"
Authentication
Authorization
Encryption


“Re-architect corporate services
to remove any privileges associated
with having a corporate network
address.”

Architecture Blueprint

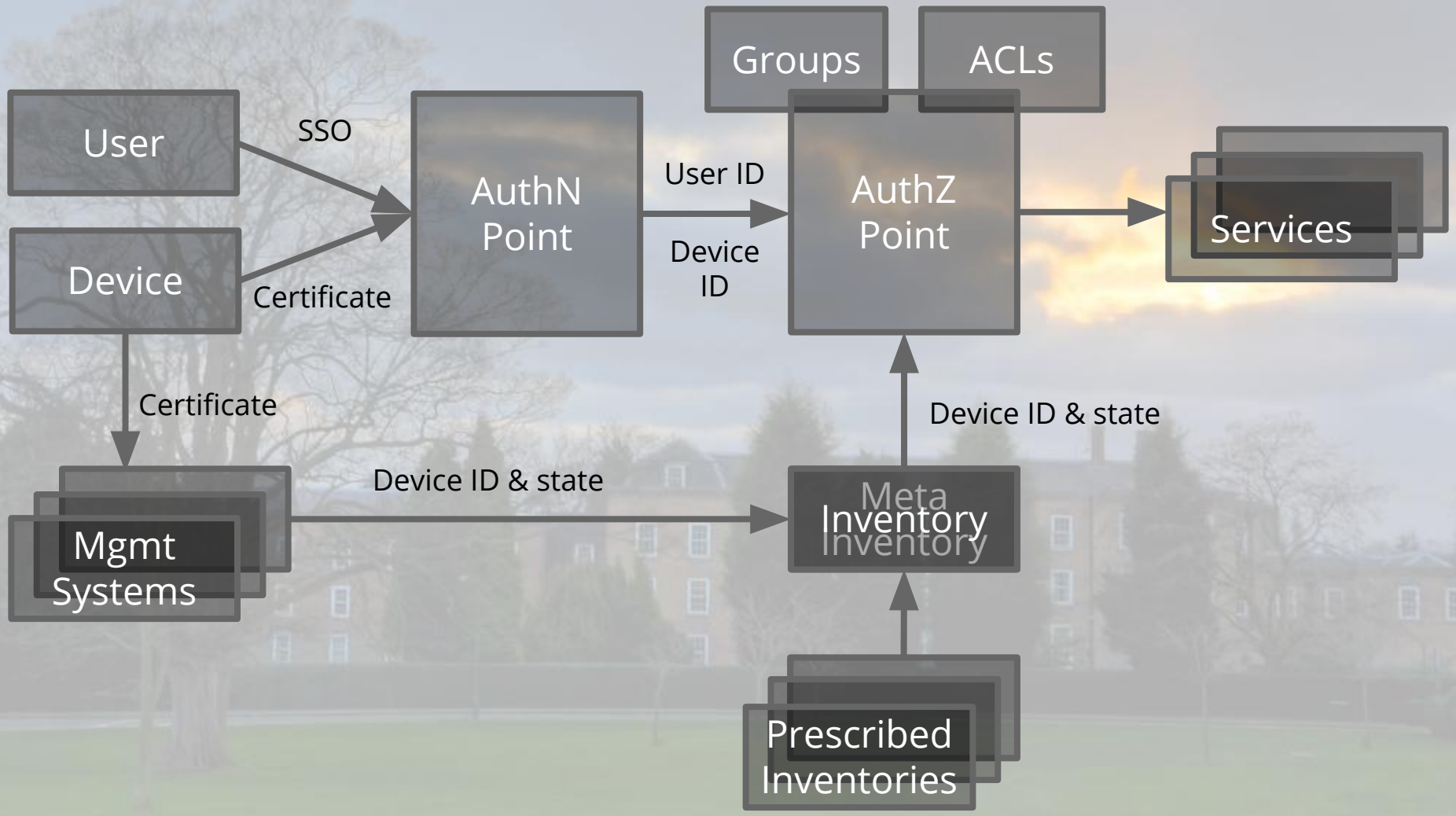
move trust to device level

device identity

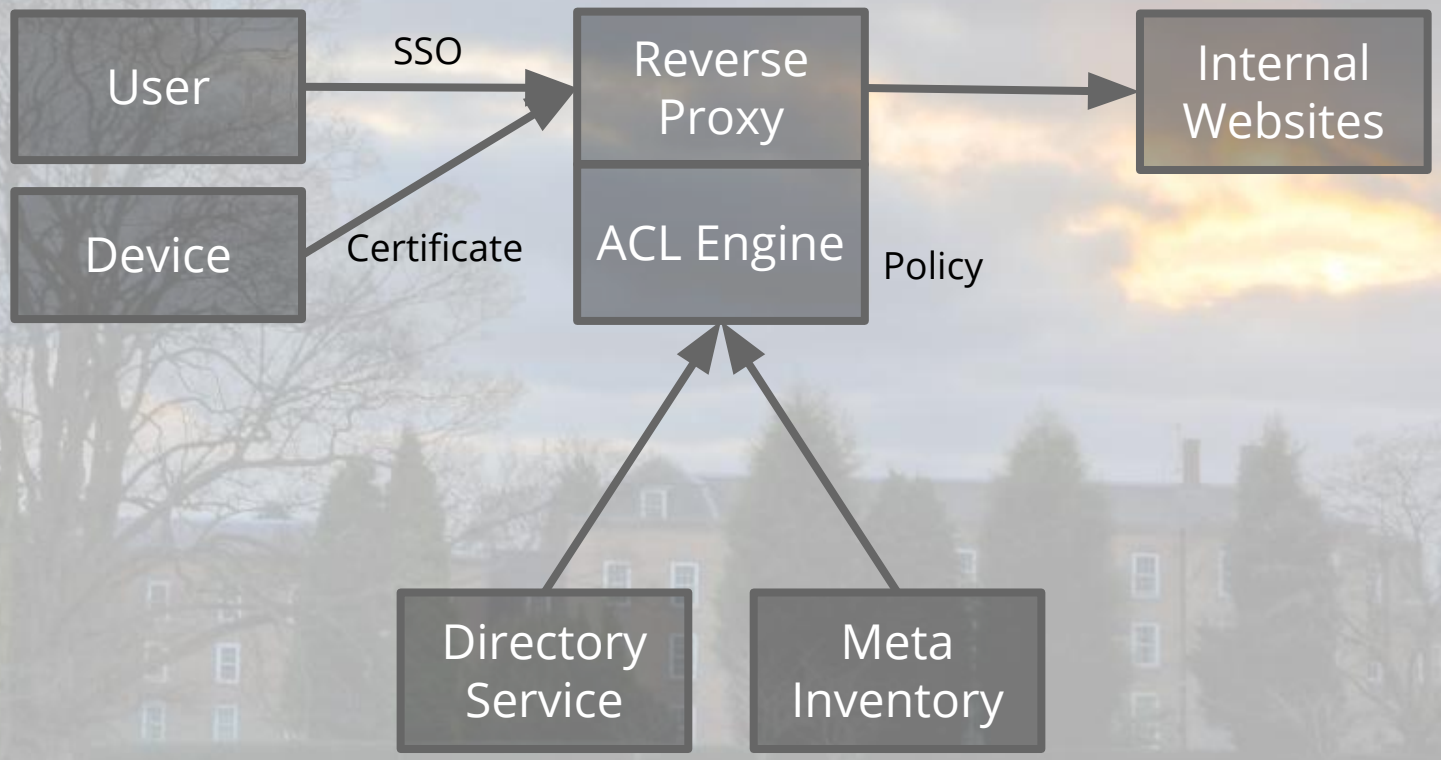
device inventory

authZ on device state

Beyond Corp Architecture



as a Reverse Web Proxy



Access Policy Examples

Payroll	Dashboard	Café Menu
Device Authentication	Device Authentication	Device Authentication
User Authentication		
Actively Managed	Actively Managed	
Patch Level Up-to-date	Patch Level Up-to-date	
Full Disk Encryption		

Rule Example - Cafe

```
(  url.hostname is 'google-menu.appspot.com'
& url.port = 443
& url.protocol is 'https'
) then permit
    named 'Menu_Permit'
    tested_by 'menu_permit_test';
```

Rule Example - Dashboard

```
(  url.port = 443
& url.protocol is 'https'
& service is 'cluster-dashboard'
& ( employee
    | intern
    | user in 'ldap/cluster-dashboard-roles'
    | user in 'group/cluster' )
& (google_managed_primary_device
    | role_managed_device )
then permit named 'cluster-dashboard' tested_by
    'cd_any_employee_from_remote_managed_device'
    'cd_any_intern_from_onsite_managed_device'
    'cd_app_engine_role_from_app_engine_device'   [etc]
```

Rule Example - Payroll ?

- No, that ACL doesn’t fit on the slide

- Why not?
  - Real world ACLs are complicated
  - Once you study the corner cases
- Need an expressive language
  - Avoid assuming user behavior
  - No broad permissive generalizations


Bootstrapping Challenges
device identity
inventory data quality
gatekeeping
dependency on user creds

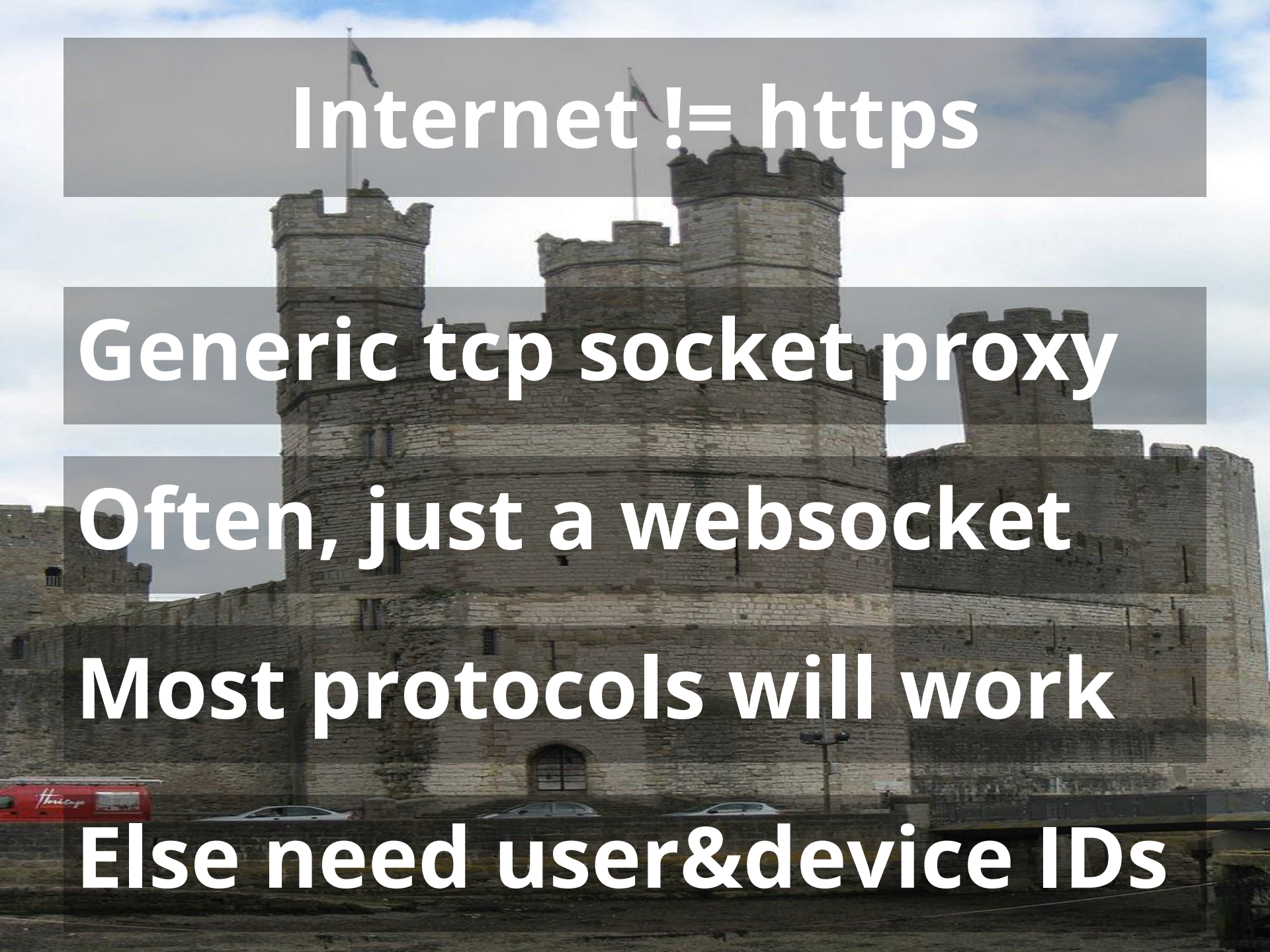
Workflow Challenges

systems management

network latency

“untrusting” the network

long tail/legacy workflows



Internet != https

Generic tcp socket proxy

Often, just a websocket

Most protocols will work

Else need user&device IDs

Advice & Directions

build support

get the data/build the gate

develop web first

Comparing the models

	Perimeter	Beyond Corp
Usability	remote access solution may be required	"It just works"
Applicability	internal network only	on all networks, including internet
Trust based on	IP Address	device ID and state
Strong attribution of access	very difficult (think NAT)	easily possible (even across tiers)
Segregation	only works on the internal network	per device/service from all networks
Inventory data quality	data quality hard to improve	much better as inventory drives the process

Questions?

http://en.wikipedia.org/wiki/Caernarfon_Castle

Images: Herbert Ortner and others