BeyondCorp

BeyondCorp

- Google Initiative
- A new approach to Enterprise Security
- http://research.google.com/pubs/pub43231.html
- Going beyond
  - perimeter security enforced by firewalls.
  - where access from outside is supported by VPNs.

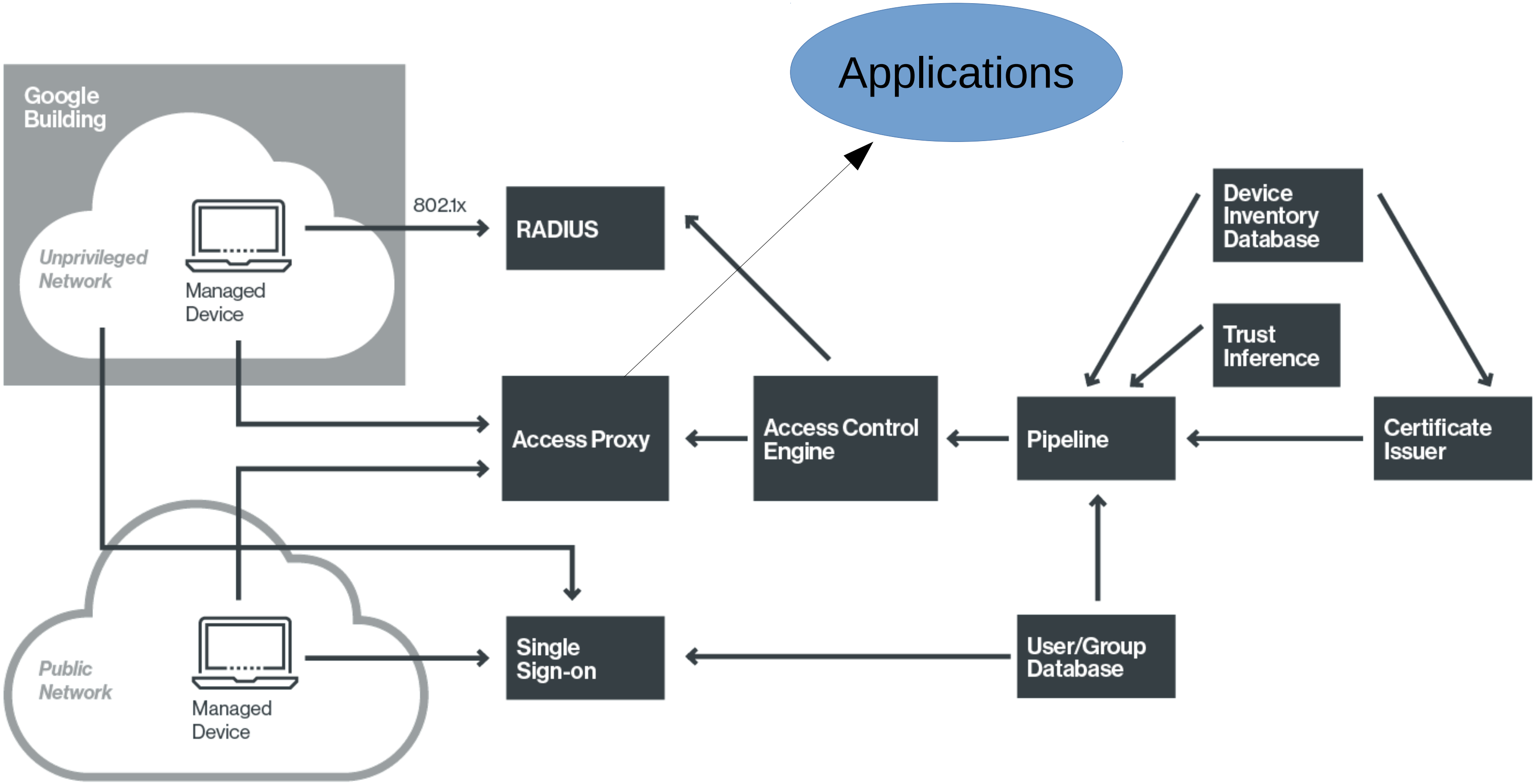
Because

- Once through the perimeter firewall, an attacker has fairly easy access to coporate intranet
- The perimeter is often no longer the physical location of the enterprise due to use of the cloud.
- Access from outside the corporate network is becoming more and more necessary.
- And is from a wide range of different devices.

The New Model

- Gets rid of the privileged corporate network.
- User access depends on the device and user credentials (and not exclusively on the location).
- All access to resources is fully authenticated, authorised and encrypted.
- No substantive difference in accessing the network from inside or outside the corporate network.

Components and Access Flow



Device Inventory Database

- A 'Managed Device' is one procured and actively managed by the company.
- Keeps track of changes (updates etc) made to these devices.
- Devices are identified by certificates stored in a Trusted Platform Module (hardware) or certificate store.

User/Group Database

- All information about users
- Usernames, job categorization, group memberships etc.
- Like users and groups in Unix.

Single Sign-On System

- Central portal to support user authentication.
- [Uses two factor authentication].
- After authentication, tokens are issued which are used when requesting resources.

The Unprivileged Network

- Clients with managed devices assigned to this network when in Google buildings.
- Unmanaged devices assigned to a guest network.
- RADIUS servers assign an IP address on the unprivileged network to a device.

Proxy

- All applications accessed through a proxy.
- Provides access control checks.
- Load balancing.
- Encrypts connection with the client.
- DOS protection.

Access Control Engine

- Supports the proxy.
- Provides authorization based on device information, user credentials and trust model.
- Level of access can change over time.
- Based on device information, user and group information, location.
- For example, a device without an important upgrade might lead to restricted access.

Pipeline

- Feeds the appropriate information into the access control engine.
- Dynamically obtains information from Device Inventory database.
- Including
  - Certificate whitelists
  - Trust levels of devices and users
- Can also carry out a certain level of trust inference.