20161004 Visitor wireless network

Attendees:

Irwin, Ben, Kent, Jeff, Bernard, Les

Current state

- Was only wireless network for many years.
- Have lot of SLAC access on visitor network
- Many users by-pass secure wireless
- May not be appropriate for SLAC business
- Does not allow/block by application policy
- Is visitor encrypted, could lead to capture of items.
- No inbound to visitor (blocked at visitor router ACL) and no intra access (i.e. no servers).
- Bandwidth to whole visitor is 1Gbps aggregate, not an issue so far.
  - Plan to upgrade to 10Gbps but a problem uses old technologies (some protocols no longer supported), needs re-architecture.
- SLAC secure wireless is 4Gbps aggregate, not a problem now based on monitoring
- Mission critical for customers who come here from offsite

Way forward

We are wrapping up perimeter project.

- Do we declare victory
  - Few months down the road do visitor
  - Then another project that may need justification
  - or do we include this under the current approved project.
  - If we do nothing how do we justify?
    - Our visitor goes through PANs and PANs block URL categories such as porn (like BlueCoats used to).
    - Can't justify as it's preferred by users to by-pass things.
  - Benefits
    - Visitor is a clumsy way for people to debug their own problem
    - They need an escape valve
  - Update visitor documentation security discussion to add
    - PAN threat protection
    - CFM application, Kent will investigate, probably, needs testing, check documentation
    - Broad Outbound connectivity
    - Anything on border ACL policy inbound or outbound?
    - Add no inbound and no servers

Need to align with Stanford.

- Causes problems to DoE visitors with Stanford filters. Maybe a router ACL.
  - Kent check what technologies are used to apply policies to the visitor, contact Dave Macia.
  - Rate limit bandwidth

Enable everyone to access secure wireless to all SLAC IDs

Enforce minimum security for unmanaged devices.

May allow a machine

LLNL treats as hotel network apart from things perceived as a threat, also some categories not allowed

LCLS has their own visitor network.

- Action item for Guillaume to see if he knows anything, also Amedeo or Veracci

Cloudpath a gateway for network, go to a captured portable and push certificate to the machine.

- How to move this forward, need Guillaume
- Does not support wired ports on visitor since they do not go through the wireless controller.
- Apple TVs (15) are therefore a concern since must be wired
  - Shows up over wireless so visitors can project via wireless

Jeff run splunk on visitor network.