draft-ietf-netconf-reverse-ssh-02

NETCONF Call Home using SSH

Recap

- NETCONF "call home" is a long time request
  - This draft enables it for SSH
  - RFC5539bis does it for TLS

- IETF 87 presentation was attended by folks from the SEC area and favorably received.

Updates from -01 to -02

- Added Applicability Statement

- Removed ZeroConf (ZeroTouch) text

- Clarified the protocol section even more

- Added a section for identification and verification

Each point discussed in upcoming slides

Applicability Statement

- Says that Reverse SSH must only be used for a NETCONF server to initiate a connection to a NETCONF client.

Removed ZeroConf (ZeroTouch) Text

RENAMED

- Per agreement in the room during the IETF 87 meeting, text regarding how to bootstrap security parameters has been removed.

- Now a separate draft for complete solution:
  - draft-kwatsen-netconf-zerotouch-00
    - Co-authored with Steve Hanna

Clarified Protocol Section

- Greatly expanded text for what exactly the network element and the management server do.

- Moved all other text into other sections, so protocol section only discusses the protocol.

New Identification and Verification Section

- Text from "Protocol section" moved here.

- This section explains how identification and verification can be achieved
  - RECOMMENDS network-elements use X.509-based host keys

YANG Module

- Reverse SSH draft defines a YANG module enabling the configuration of necessary parameters on network elements.

- This YANG module was used to validate sample configuration files for the Reverse SSH reference implementation

Should repurpose grouping with the TLS draft's YANG module?

IPR

- Filed by Juniper for an awarded patent

- Reasonable Non-Discriminatory terms, with termination on conflict

Reference Implementation

- Code is developed
- Going through internal review…

Port Issue

- Currently there is some question regarding if the Call Home mechanisms for SSH and TLS warrant new IANA-assigned ports.

- Options:
  - Continue to push for a port
  - Rewrite drafts to not require a default port
  - Update SSH & TLS drafts with a reversal flag

Questions / Concerns ?