draft-ietf-netconf-reverse-ssh

Call Home using SSH

Motivation

- Proactive device-initiated discovery
- Manage devices deployed behind firewalls

SSH is NETCONF's mandatory transport protocol

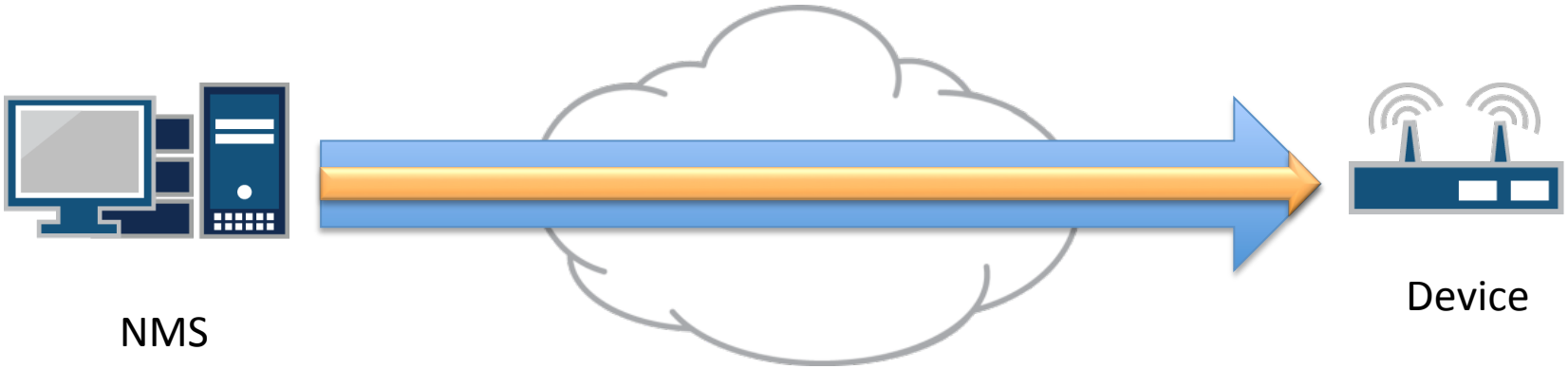
Normal SSH

- SSH client initiates the TCP connection…

NMS initiates TCP connection

Normal SSH

- SSH client initiates the TCP connection…



SSH on top of TCP connection

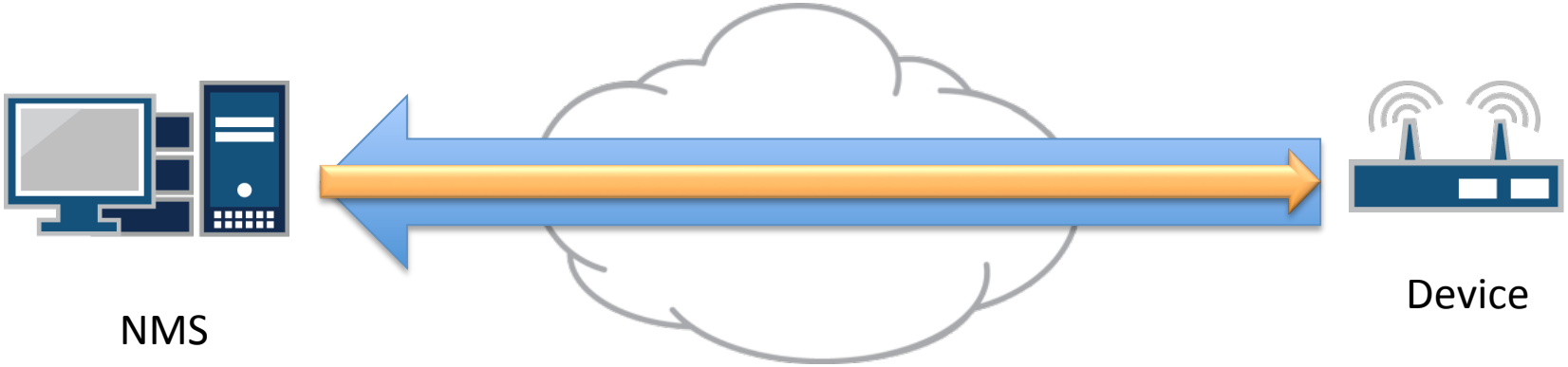
Reverse SSH

- Device initiates the TCP connection…

Device initiates TCP connection

Reverse SSH

- Device initiates the TCP connection…



SSH on top of TCP connection

SSH Roles are Always the Same!

Regardless which side initiates the TCP connection:

- NMS is the SSH client
- Device is the SSH Server

Security wise:

- NMS authenticates device's SSH host key
- Device authenticates NMS's "user" credentials

RFC 6242 Compliant

- NETCONF server extracts username from ssh-userauth service
- NETCONF client opens session channel and invokes "netconf" subsystem

Very Easy to Implement

Normal SSH

- `inetd` listens on a port 830
- Accepts TCP connection
- Forks/execs “sshd -i”

Reverse SSH

- Agent on device initiates TCP connection to NMS on port TBD
- Forks/execs “sshd –i”

Reference implementation will be posted
- using OpenSSH and J2SSH Maverick

Bootstrap Parameters

- Devices must be configured
  - the IP/port of the NMS to initiate connection to
  - A user account and credentials for the NMS to use
- NMS should be configured
  - Identities for expected device connections
  - Device SSH Host Keys
    - or an ability to authenticate devices (e.g. PKI)

Zero-Touch Bootstrap

Automated configuration of Bootstrap Parameters from previous slide

- A highly-requested feature

- Device bootstrap procedure
  - Device placed on isolated network
  - Device configures its network stack via DHCP
  - Device fetches Bootstrap Parameters from network

- Security Recommendations
  - NMS's "user" credentials SHOULD be an asymmetric key
  - Device's Host-Key SHOULD be a X.509 certificate

Regarding X.509 Based Keys

- RFC 6187 defines
  - X.509v3 Certificates for Secure Shell Authentication
  - March 2011
- Currently no known implementations
  - some implementations of draft-saarenmaa-ssh-x509-00
- Following are planning to support
  - The OpenSSH patch by Roumen Petrov
  - J2SSH Maverick by SSHTOOLS Limited

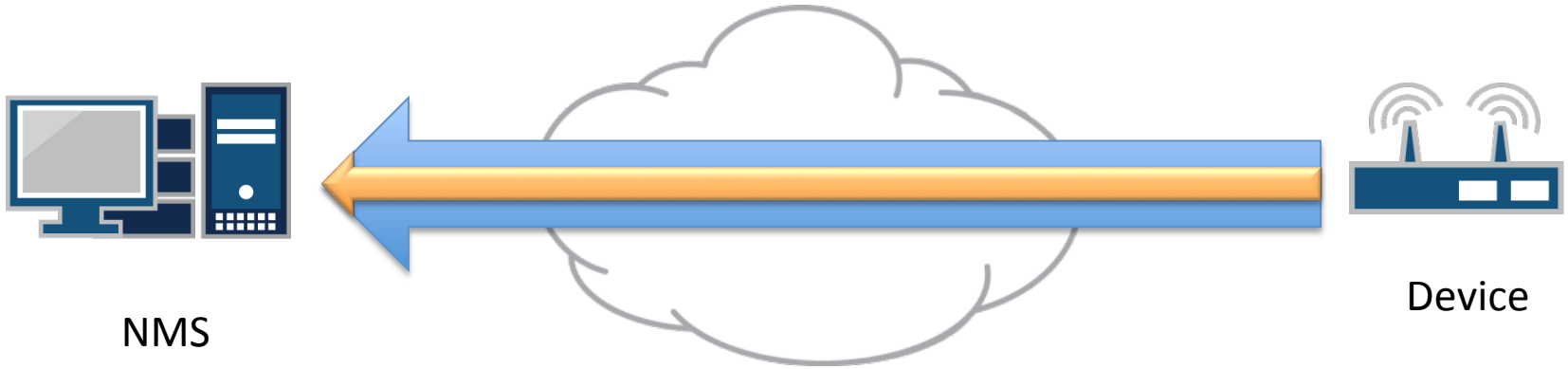
Questions / Concerns ?

Alternative Strategy

- Device is SSH Client

Alternative Strategy

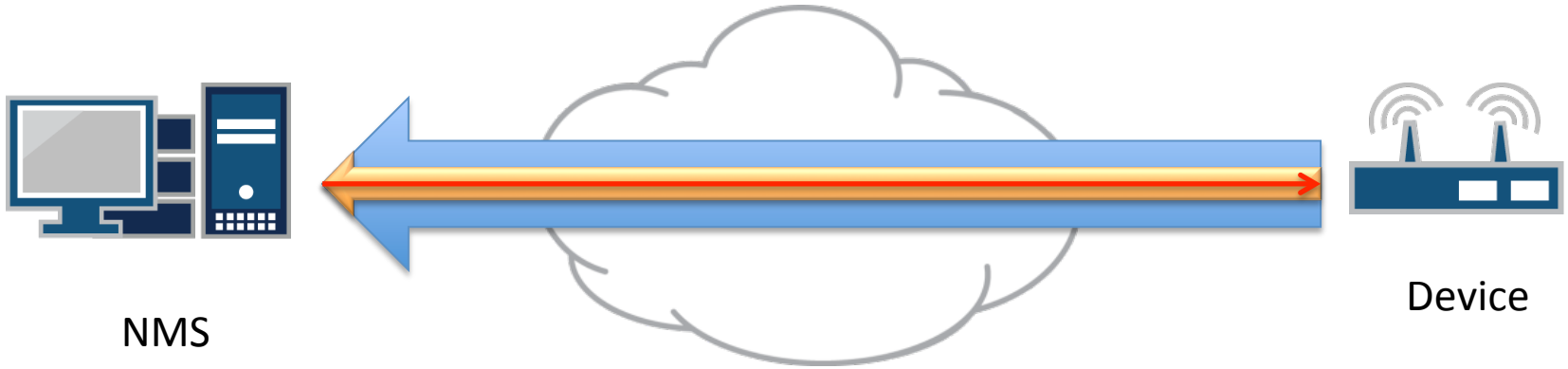
- Device is SSH Client



SSH on top of TCP connection

Alternative Strategy

- Device is SSH Client



NMS opens channel on device

Bootstrap Parameters

- Devices must be configured
  - the IP/port of the NMS to initiate connection to
  - NMS's SSH Host Key
    - or an ability to authenticate it (e.g. PKI)
  - A user account and credentials to log into the NMS
  - A local user account to bind session to