FIXED NETWORK ACCESS DEVICE (FNAD)-SUPPLY CHAIN MONITORING CENTER (SCMC) CONNECTIVITY ALTERNATIVES AND SITE FIREWALL CONSIDERATIONS

Note: 1. Each NAD may use one of the alternatives listed below. Other alternatives maybe identify after the discussions with site IT staff. Connectivity among NADs may differ due to their locations.

2. Case numbers shown below correspond to the included FNAD Network single page table.

3. Case 4a and Case 4b connectivity maybe shared among one or more FNADs

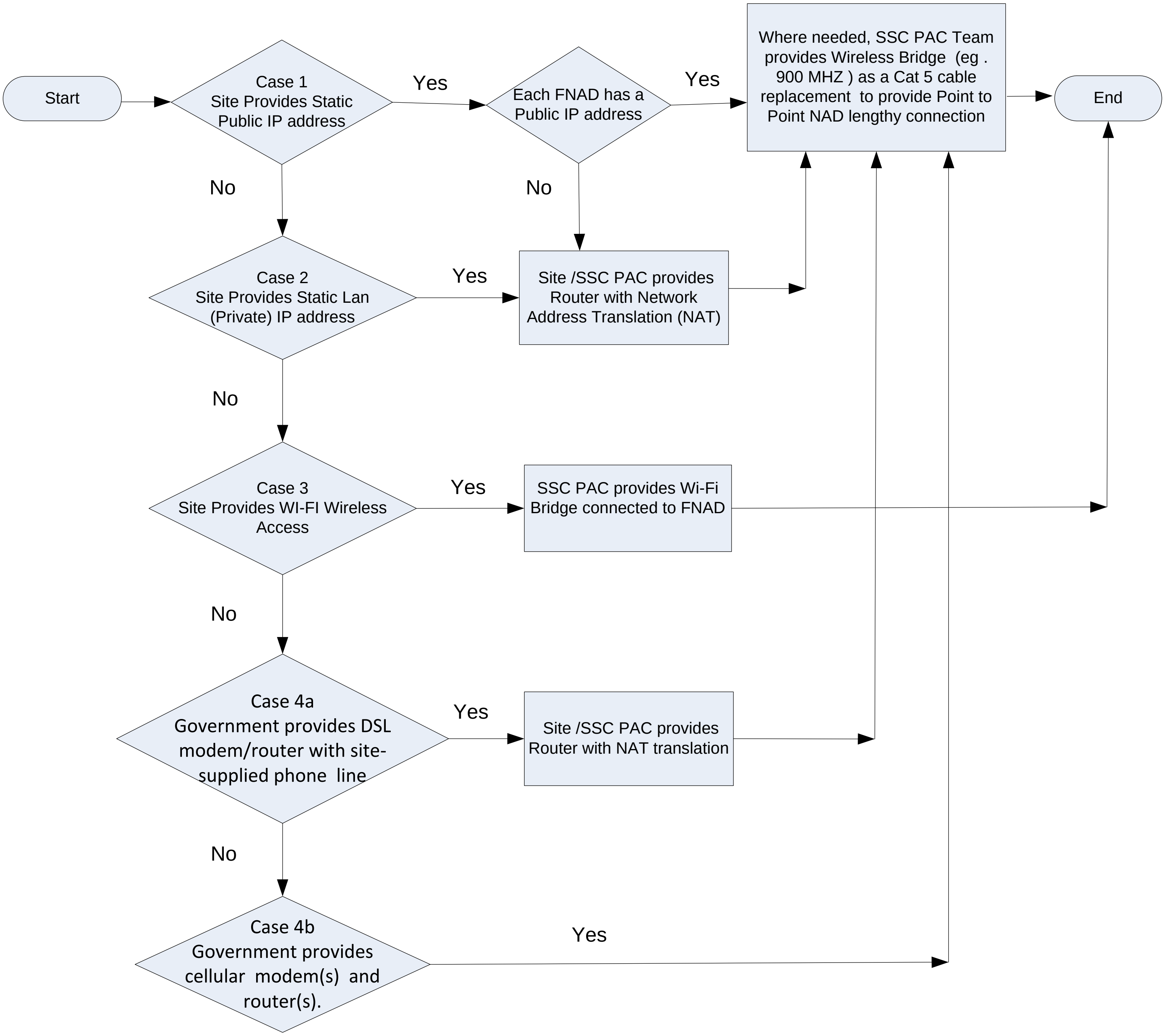
*** The following ports are used. For solutions that use the host site network, the site's firewall needs to accommodate. The specific port numbers shown below can be changed during the FNAD configuration.**

Port X out : ICD compliant UDP or TCP message traffic between FNADs and SCMC

Port 514 out– used for SYSLOG client remotely send FNAD status to SYSLOG sever

Port 20 (FTP client passive mode) out: -used to remotely update of the FNAD firmware

Port 13 out- used for FNAD to retrieve UTC time which is included in the NADA (Network Access Device Announcement) message



Start
Case 1
Site Provides Static
Public IP address
Yes
Each FNAD has a
Public IP address
Yes
Where needed, SSC PAC Team provides Wireless Bridge (eg . 900 MHZ) as a Cat 5 cable replacement to provide Point to Point NAD lengthy connection
End
No
No
Case 2
Site Provides Static Lan
(Private) IP address
Yes
Site /SSC PAC provides Router with Network Address Translation (NAT)
No
Case 3
Site Provides WI-FI Wireless
Access
Yes
SSC PAC provides Wi-Fi Bridge connected to FNAD
No
Case 4a
Government provides DSL
modem/router with site-
supplied phone line
Yes
Site /SSC PAC provides Router with NAT translation
No
Case 4b
Government provides
cellular modem(s) and
router(s).
Yes

Planning: Fixed Network Access Device (FNAD) To DCP Connectivity 8/30/11 slc

COMMUNICATION ACTIVITY	DATA EXCHANGE	DATA VOLUME	PROTOCOL TYPE	PROTOCOL PORT(s) USED	SITE FIREWALL CONSIDERATIONS *Cases* are WAN connectivity alternatives
ICD COMPLIANT MESSAGE TRAFFIC	One or more FNADs Data traffic to/from one server at the Data Center (DCP)	Very low. When container enters coverage, a small number of packets are exchanged with the DCP.	Choose TCP or UDP per the ICD.	An FNAD accepts traffic DCP traffic on a chosen port number. DCP accepts TCP or UDP traffic on one port number for all FNADs.	**Case 1: Site-supplied Public IP Address:** FNAD(s) are given a public IP address. Firewall passes traffic to the FNADs' IP, on all port numbers or only the required port numbers shown in this table. **Case 2: Site-supplied LAN IP Address:** FNAD(s) are given a static IP LAN address and router does NAT. Firewall does *port translation* for traffic to/from the FNADs' IP, on only the required port numbers shown in this table. **Case 3: Site-supplied WiFi Access:** FNADs use site's "visitor" access to Site's WiFi network for Internet-only access. Ports defined in this table are open. **Case 4a: Government provided DSL modem/router with site-supplied phone line**: Site's firewall not used. Can be shared among FNADs. **Case 4b: Government provided cellular modem/router.** Site's firewall not used. Can be shared among FNADs.
FNAD FIRMWARE UPDATE	FNAD to remote firmware update server. Server logins are enabled briefly, when necessary.	Infrequent file transfer for remote firmware updates. File size ~250KB	TCP, FTP w/passive mode. FNAD initiates connections.	21 (per standard) or chosen alternative, and Chosen port no. for data (FTP passive mode)	Same as above
FNAD STATUS MONITORING	FNAD to designated administrative log storage server One-way data flow.	Very low. A few packets per hour	UDP/SYSLOG (RFC standard)	514 per standard) or chosen alternative	Same as above
FNAD CONFIGURATION MANAGEMENT	FNAD login from authorized remote user PC. Uses anti-replay login with auto-ban.	Infrequent changes to configuration	HTTP	80 or chosen alternative	Same as above