Securing Your Network

Whether you are installing a Sangoma NSG appliance or the NSG Software version on your own hardware, securing your network is paramount. Any security breaches can cost thousands of dollars of toll fraud and can compromise entire networks.

Although NSG has some firewall capabilities, it is not designed to fully secure your network from intrusion and hackers. It is your responsibility to keep your network secure with other hardware devices, such as a Session Border Controller (which Sangoma can supply).

Once you have taken the appropriate security considerations, continue to the Appliance Installation or Software version Installation (whichever applies to you).

There are two areas in your network that require you to secure:

- The SIP network that connects to NetBorder SS7 Gateway
- The SS7 Network that connects to NetBorder SS7 Gateway

See below for a general network setup to better understand the two areas (circled in Red ovals):

**Securing the SIP network that connects to NetBorder SS7 Gateway**

Securing the SIP Network that connects to the NSG Gateway is the most vulnerable area in terms of security risks.

- The most basic way to secure the SIP Network is to configure the SIP network to register to the NSG Gateway. By doing this, NSG will only accept calls from the trusted registered SIP Network device(s) and block/drop all other call attempts.
  - Registering your SIP network to NSG is trivial. If you an Asterisk or FreeSWITCH based PBX on the SIP Network, please follow these step-by-step instructions: [Third Party Integration](#)

Beyond the above approach, Sangoma recommends the installation of a Session Border Controller (SBC) appliance between the NSG Gateway and the SIP network devices. This will provide full security protection against all threats. Whether you purchase an SBC from Sangoma or a third
If you install an SBC to protect your SIP network, configure the NSG Gateway in registration mode, as detailed in the previous step. This will have the NSG Gateway trust only the SBC for call traffic, where the SBC will protect the entire SIP network from attacks.

**Securing the SS7 network that connects to NetBorder SS7 Gateway**

Since the SS7 Network physically connects to the NSG Gateway via E1/T1 cables from the telco, the security concerns are minimal when compared with the SIP network. This is because the telco takes care of securing their call traffic which then only reaches your NSG Gateway via the E1/T1 cables. This being said, good practice is to still secure your network in the case there is a security breach between the telco and the NSG Gateway.

To protect the SS7 Network the best method is to customize the NSG Gateway dial plan to accept calls only from specific country codes, call patterns..etc. For dial plan customization please contact our Support team at support.sangoma.com