Securing your Enterprise Network with SBC

Scott Beer

Director Solutions Engineering, Sangoma

Switchvox Today

- Leverages the Security Features of a Firewall
- Firewall Settings
  - Port Forward VoIP ports (i.e. 5060)
  - Allow access from ITSP IP address and remote clients and block everything else
- Switchvox Settings
  - Configure Access Control List Rules
  - Very Strong extension & voicemail passwords
  - Restrict Admin GUI to known IP address ranges

FreePBX/PBXact Today

- Leverages the Security Features of a Firewall
- Firewall Settings
  - Port Forward VoIP ports (i.e. 5060)
  - Allow access from ITSP IP address and remote clients and block everything else
- FreePBX/PBXact Settings
  - Enable Responsive Firewall
  - Define Known Networks List Rules
  - Very Strong extension & voicemail passwords
  - Restrict Admin GUI to known IP address ranges

Why are we talking about SBCs

- Security and Protection of business phone systems is Important
  - Don’t Under value the need to have VoIP Security
- Ask! – What is your Security Policy?
  - Firewalls provide Data Security solutions
  - SBCs compliment Firewalls for VoIP Security solutions
- SBC provide additional VoIP Security into a network

Why are we talking about SBCs

- Security and Protection of Your VoIP environment is not trivial
  - Can’t protect your entire network by implementing only one method
  - Hackers only need one exposed area of your network to take it all down
- Malicious activity caused by hackers is growing and businesses are being compromised
  - Because business owners are not educating themselves about VoIP security.
  - The transition from legacy phone system environments to VoIP environments is creating an increasing gap of ignorance, benefiting hackers
    - The ubiquitous network firewall is no longer the one-stop shop for protection, as in ‘the old days’. They protect ONLY your data
    - Hackers are hoping that you don’t know that your VoIP network is an open door

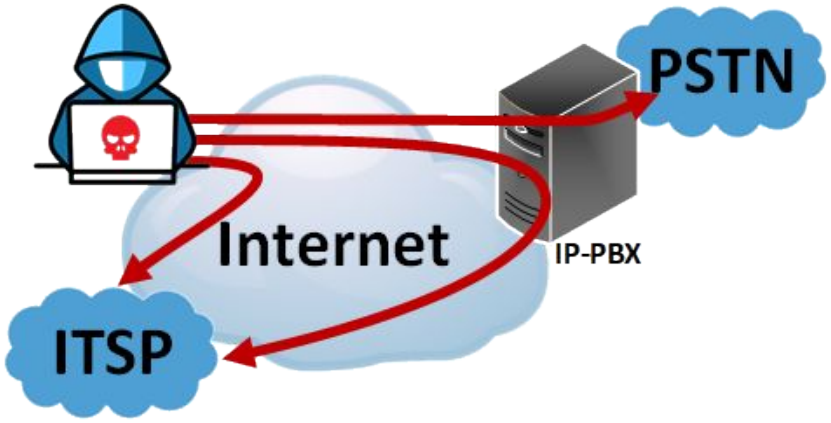
Why are we talking about SBCs

- Security and Protection is a layered approach
- Create multiple roadblocks for hackers that together form an entire shield
- Maintain your protection methods too! Have policies in place to routinely check and monitor
- We will show you how to create a layered protection approach with Sangoma SBCs to form a rock solid shield against hackers

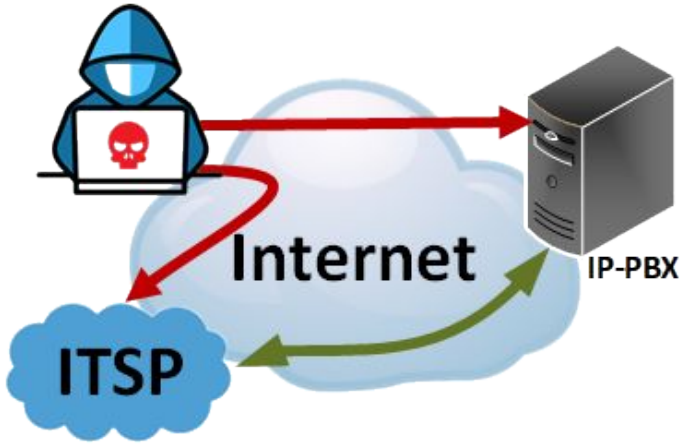
- SBCs Compliment existing Security infrastructure, by adding VoIP specific security policies to the Firewall.

Types of Attacks by Hackers

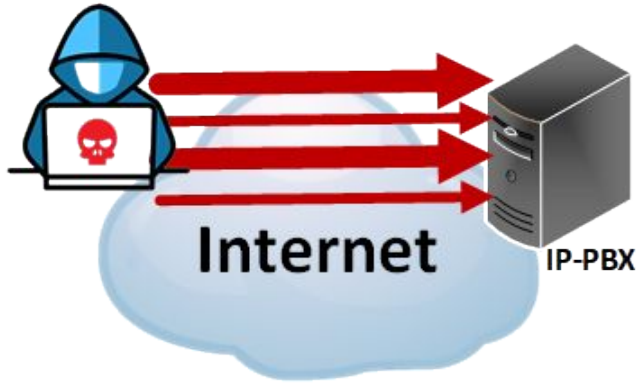
- Toll Fraud



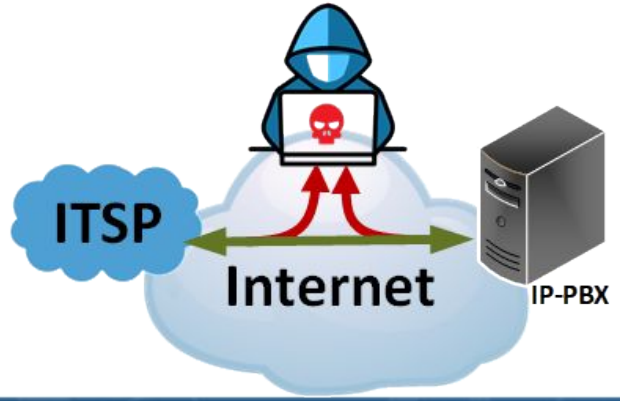
- Identity Theft



- Denial of Service



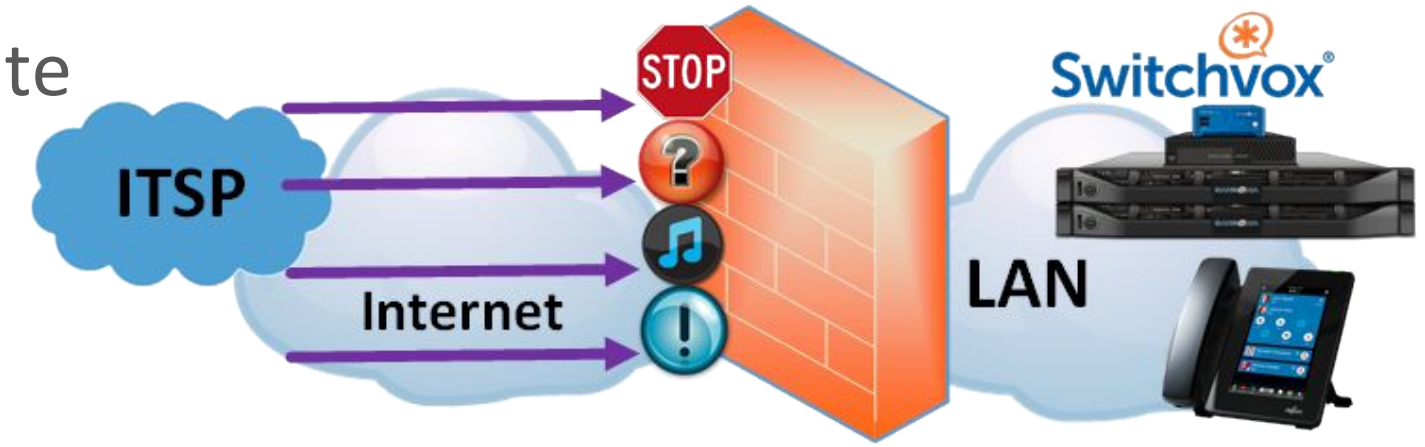
- Eavesdropping



Firewalls are Not Enough

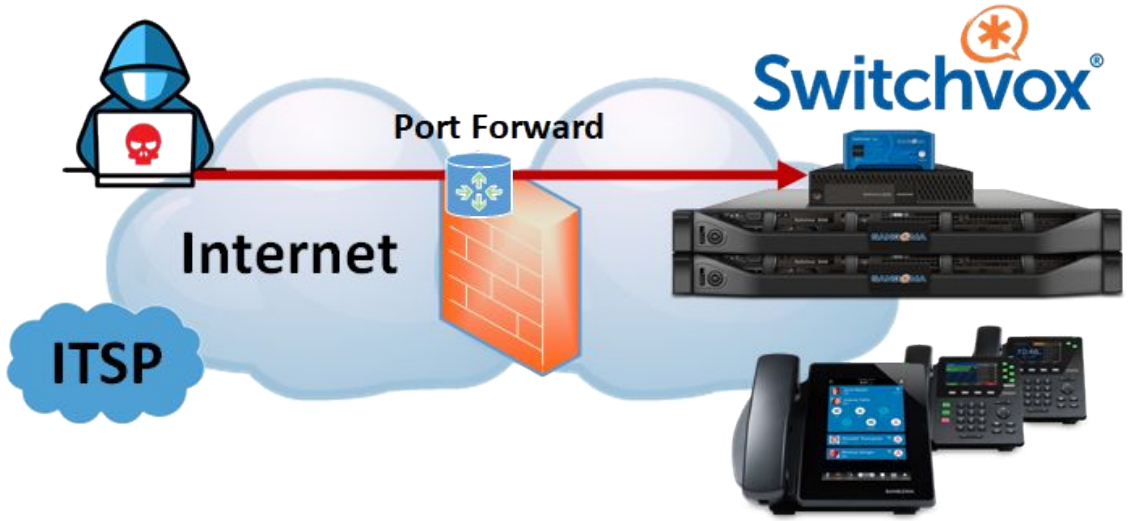
- Firewalls were never designed for VoIP traffic
- Inherent function is to Deny ALL unsolicited traffic
- Do Not understand SIP protocol and routing needs (SIP is the protocol used for VoIP)
- Audio Media requires separate negotiation
- Not setup for Real Time communication

- Won't a SIP ALG work?
  - NO. They understand SIP, but do not apply Security policies



Firewalls are Not Enough

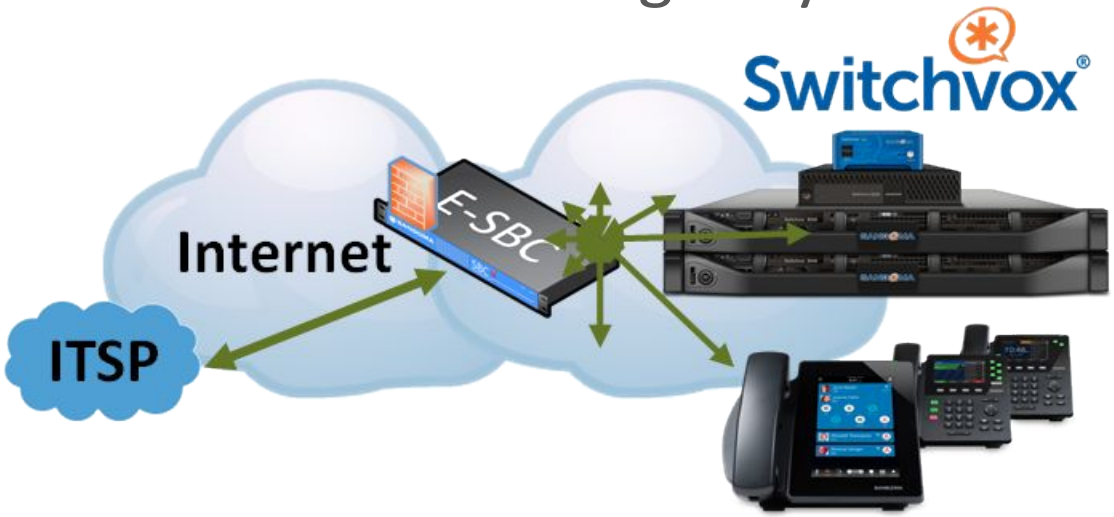
- Work around when using a firewall for VoIP: “Poking Holes” to allow VoIP Traffic through – SIP and Audio/Video
  - This is why businesses get hacked!



- Cons
  - IP-PBX must deal with VoIP Security threats directly
  - Requires some Firewall configuration knowledge
  - Poking Holes in Firewall to route. insecure traffic into a Private Network

The SBC is the Solution

- SBC's are not well understood and require some VoIP education
- If you create a data network, you buy a firewall
- If you have a VoIP network you buy an SBC
- SBC is a device placed at the edge of your VoIP network, which monitors ALL of the VoIP traffic going in and out
- Based on the type of traffic it will intelligently make decisions to block/deny, re-route...etc.



SBC Features

- Security:
  - Protect from denial of service attacks (DoS or DDoS), fuzzing, and toll fraud
  - ACLs
  - SIP Protocol Filtering and Rate Limiting
  - SIP Protocol IDS/IPS
- Encryption:
  - Prevent eavesdropping and authenticate the call end points
- Registration Policy:
  - Prevent unregistered end points from getting access to your VoIP service
- Call Routing:
  - Provide dynamic routing
  - Survivable and Resilient Routing
  - Least cost routing and load balancing
- SIP Conversion:

SBC Use Cases

SANGOMA

Use Cases

- **Remote Workers**
- **SIP Trunking**
- SBC for TDM Support
- Virtual SBC
- Transcoding
- Security
- High Availability
- Interoperability

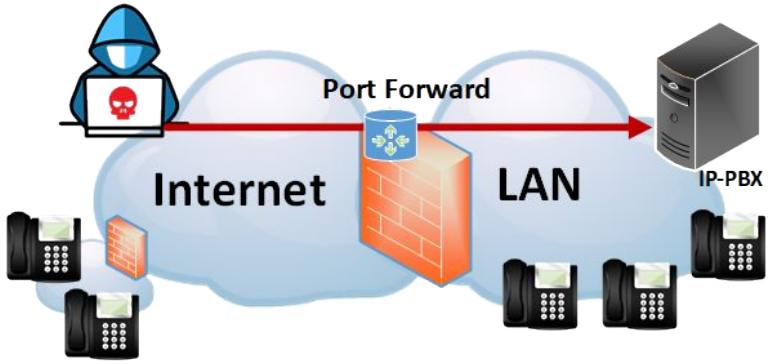
Remote Worker

- Most popular Request by many customers using a SIP based IP-PBX
  - How do we secure remote SIP phones?
- Allows access to authorized endpoints on remote worker premises. Eliminate interoperation and firewall issues on corporate and remote worker networks, maintain security.
- Features
  - No VPN required
  - Pass-through SIP registration
  - Remote FW/NAT traversal
  - Call Admission Control
  - Topology Hiding
  - TLS and SRTP encryption

- Use of SBC is Not yet supported on Switchvox for Remote D Phones and Softphones
- Zulu does use SBC

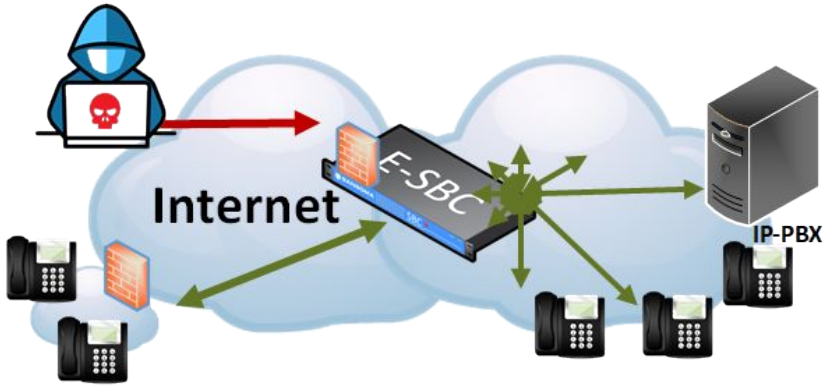
Remote Worker

- Without an SBC



- Firewall - Open Ports to allow SIP Application through
  - And other Port for needed applications
- This moves the Security responsibility to the IP-PBX

- With an SBC

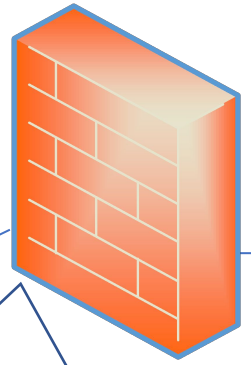


- SIP Calls through the SBC, which is able to detect and handle any attacks
- Adds a layer of Control

Remote Worker Configuration

Internet

Remote SIP Phones



- SBC is “Best in Class” SIP (VoIP) Security

SBC

- Configure to accept only SBC IP address
- User/Pw Authenticate SIP

Generic SIP IP-PBX

- Firewall is “Best in Class” traditional Security
- Send phones to SIP port
- Port forward SIP port to the SBC

IP-PBX will add another layer of self protection.

Does not have to be “Best in Class” Firewall and SBC as well as a PBX

SIP Trunking

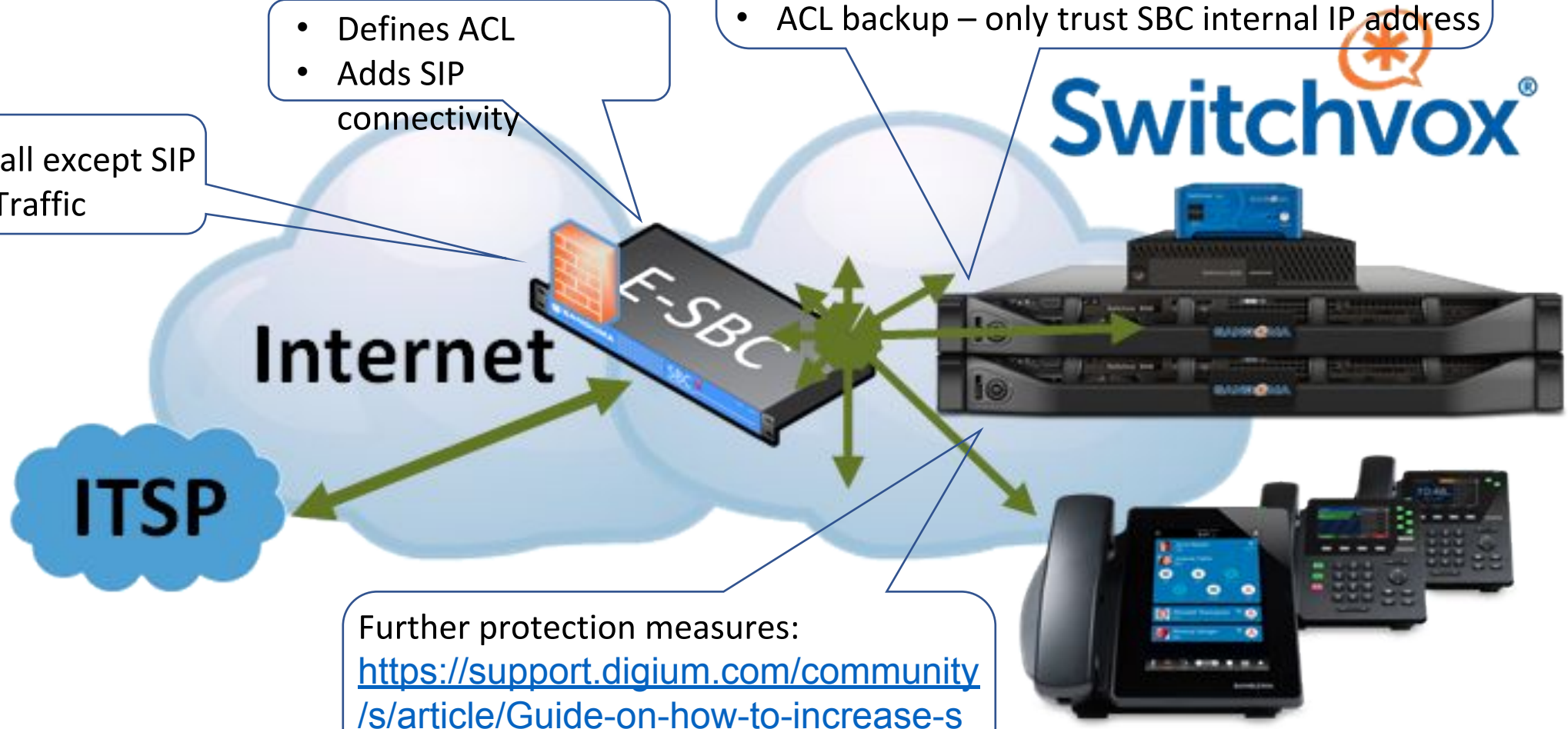
- Reduce costs of local and long distance dialing charges by using VoIP delivered via SIP trunks
- The SBC provides a defined demarcation point between the internet telephone service provider (ITSP), and the enterprise's corporate network
  - Provides VoIP Security
  - Solves Interoperating issues
  - Provides Media Transcoding

SIP Trunking Configuring

- VoIP Provider is now the SBC
- Inbound calls is SBC (VoIP Provider)
- Outbound calls use SBC (VoIP Provider)
- ACL backup – only trust SBC internal IP address

- Defines ACL
- Adds SIP connectivity

- Deny all except SIP VoIP Traffic



Further protection measures:
https://support.digium.com/community/s/article/Guide-on-how-to-increase-security-your-Switchvox-PBX

DataCenter SIP Trunking Configuring

- Multiple Carrier Support

- Hosted Phones through Firewall

- Defines ACL
- Adds Trunk connectivity
- Trunk DID Distribution

Multiple IP-PBX Instances

Why You Win with Sangoma SBC

- Ease of Installation and Use
  - Simple Licensing
  - Straight Forward Configuration for complex solutions
- Security
  - Numerous features such as IDS/IPS, ACL, Filtering and more
- Flexibility in Deployments
  - Robust Routing
  - High Availability solutions
  - Flexible network deployment configurations

FAQ

- Why do you need an SBC in the SIP trunking use Case? Can't you use the Switchvox ACL and lock down the IP to the trusted ITSP?
  - If someone spoofs the IP address they can start hacking and compromise Switchvox
  - Giving the ACL control to the SBC ensures the SBC handles the attacks. You can still use ACL in Switchvox as second layer of defense and lock the IP to the SBC
  - Easy MSP deployments – Carrier and Call Distribution

FAQ

- Training
  - Free online SBC training available at training.sangoma.com
- Documentation
  - Sangoma.com – sales and marketing collateral
  - Wiki.sangoma.com– technical instructions
    - Step-by-Step configuration guides available to setup SBC
- Configuration
  - Remote configuration available through support staff from portal (support.sangoma.com)
  - Recommendations
    - Remote Installation Support – 8 hour block
      - Some installations will require less hours due to simplicity and network
- Maintenance
  - All SBCs require annual maintenance plans for any support requests
  - Support credits are required in order to receive assistance
  - Hourly blocks purchased through support.sangoma.com

Sangoma SBC Family

- **SMB SBC**
  - 5-30 Sessions/Calls

- **Enterprise SBC**
  - 25-250 Sessions/Calls
  - TDM Inferface version

- **NetBorder SBC**
  - 250-4000 Sessions/Calls

- **VM Enterprise SBC**
  - 25-1000 Sessions/Calls
  - Software Only/Virtual Machine Ready

Thank You! Contact us.

sangoma.com

sbeer@sangoma.com

905-474-1990 x4150

SANGOMA