Remote Office Connection without VPN Use Case

SANGOMA USE CASE

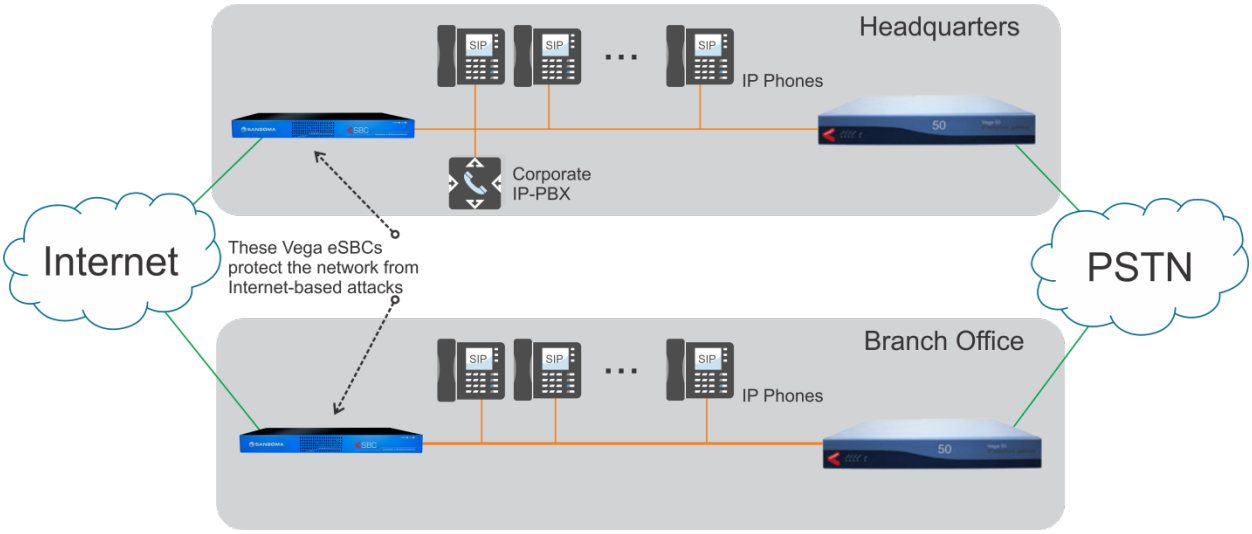

Figure 1: Branch office and headquarters VoIP LANs interconnected across the internet

The cost of maintaining dedicated telephone connections between branch offices and headquarters can be significant. Each branch office needs a dedicated multiline voice connection to the main office, typically T1 or T3. A connection between each branch office may also be required.

If all branches need to be interconnected, an ever increasing number of connections are required. For example, a single branch office (two locations) requires one connection, two branch offices require three connections, and nine branch offices (10 locations) require 45 connections.

A centrally located IP-PBX cluster can manage all voicemail and another telephone functions for headquarters and for all branch offices. Connectivity between each branch office and the central IP-PBX is achieved through the internet. A limited number of local PSTN connections can be retained for business continuity in the event of a failed internet connection.

The challenge to extending the VoIP system across the internet between branches and headquarters is ensuring security for the network and privacy for conversations. One way to achieve these security functions is by protecting intraoffice communications with a VPN. However, this requires one VPN account per trunk, which requires powerful VPN servers when large numbers of locations are involved. VPN connections add overhead to the internet connection which consumes bandwidth. Upgrades and additional configuration to routers, firewalls, and other network components may be required to obtain a fully

100 Renfrew Drive, Suite 100, Markham ON L3R 9R6 Canada
☏ +1 905 474 1990 or 1 800 388 2475 (toll free in N. America) ✉ sales@sangoma.com
SANGOMA
sangoma.com

functional and efficient VoIP system. VPNs can be tedious to setup for a VoIP system, and may require special configuration for each user.

An alternative to using VPNs to secure the VoIP system between offices is to deploy SBCs to interconnect VoIP LANs across the internet. SBCs are installed at the edge of each LAN and work transparently, with no need to configure individuals' equipment. This requires less powerful servers and much less configuration and management compared to VPNs. The SBC protects the network from security threats, and can offer voice encryption, increasing the level of voice privacy.

Firewalls and Network Address Translation (NAT) impede the flow of VoIP traffic between the corporate network and SIP trunks. An SBC is the best way to solve these network transversal challenges because it allows VoIP traffic to pass between the corporate LAN and the internet without exposing the corporate network through the opening of ports in the firewall.

Although SIP is a standard, the many ways in which it can be implemented can lead to incompatibilities between SIP devices such as phone handsets from a variety of vendors, the IP-PBX, and the SIP trunk provider. The SBC normalizes SIP, transparently translating each variety of SIP into the appropriate format for each device.

Using an SBC to manage intraoffice voice connections offers a robust solution with lower equipment costs, and with less disruption to the network and to users, than using a VPN to accomplish the same thing.

For a typical small-to medium-sized business installation, the Sangoma eSBC has ample capacity to handle the call load. For large call volumes, the Sangoma carrier-class NetBorder SBC may be more suitable.

In cases where SIP trunks are installed for outside telephone connections, each office location can connect directly to the PSTN using of VoIP gateway such as the Sangoma Vega series.

100 Renfrew Drive, Suite 100, Markham ON L3R 9R6 Canada
☏ +1 905 474 1990 or 1 800 388 2475 (toll free in N. America) ✉ sales@sangoma.com