Tadiran Telecom

10/2007

Application Notes

Sentinel Pro

Introduction

Many remote workers need to communicate with their company. Voice over IP allows remote workers to be connected to the office. However, data security becomes an issue for a company when it deploys remote VoIP.

The Coral Sentinel Pro is a Session Border Control (SBC) solution enabling the connection of remote IP phones that are located behind NAT (Network Address Translation) servers or firewalls without the need of VPN software or hardware. Its main purpose is to transfer signaling and RTP traffic through the firewall or NAT server to the relevant endpoints in the LAN network.

The Coral Sentinel provides the following features:

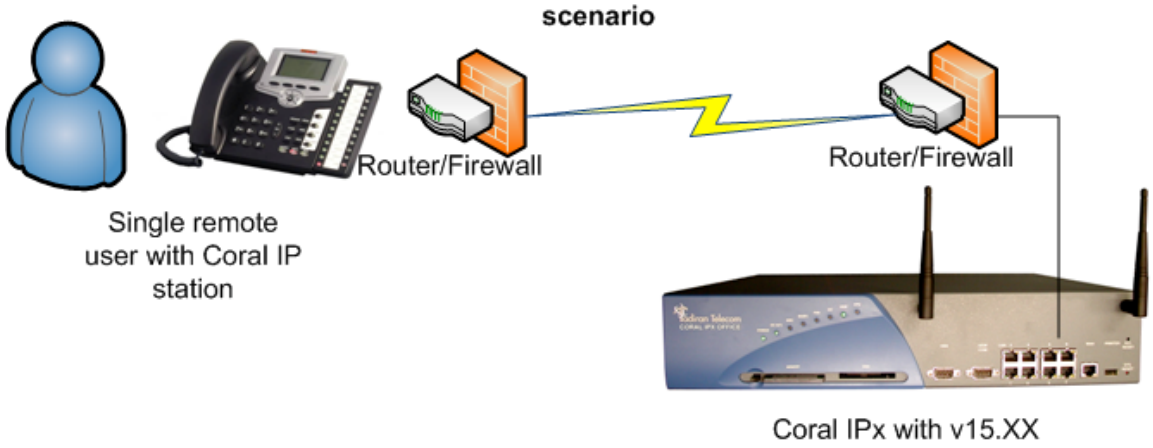
- Enables incoming traffic to be routed through a firewall, without the need to open up a permanent channel to transmit and receive calls
- Enables IP endpoints that are remotely located behind a NAT server to traverse the server
- Establishes local RTP sessions between remote IP endpoints located behind the same NAT server, thereby freeing up Sentinel RTP resources

The Sentinel Pro supports both Coral MGCP protocol and open standard Session Initiated Protocol (SIP) for terminals and stations.

Single Remote User – Home or Wireless

In a certain configuration with Coral, a Sentinel Pro is not required. That is when the remote user is the only remote IP device talking to the Coral.

Figure 1 – Single home or remote user scenario



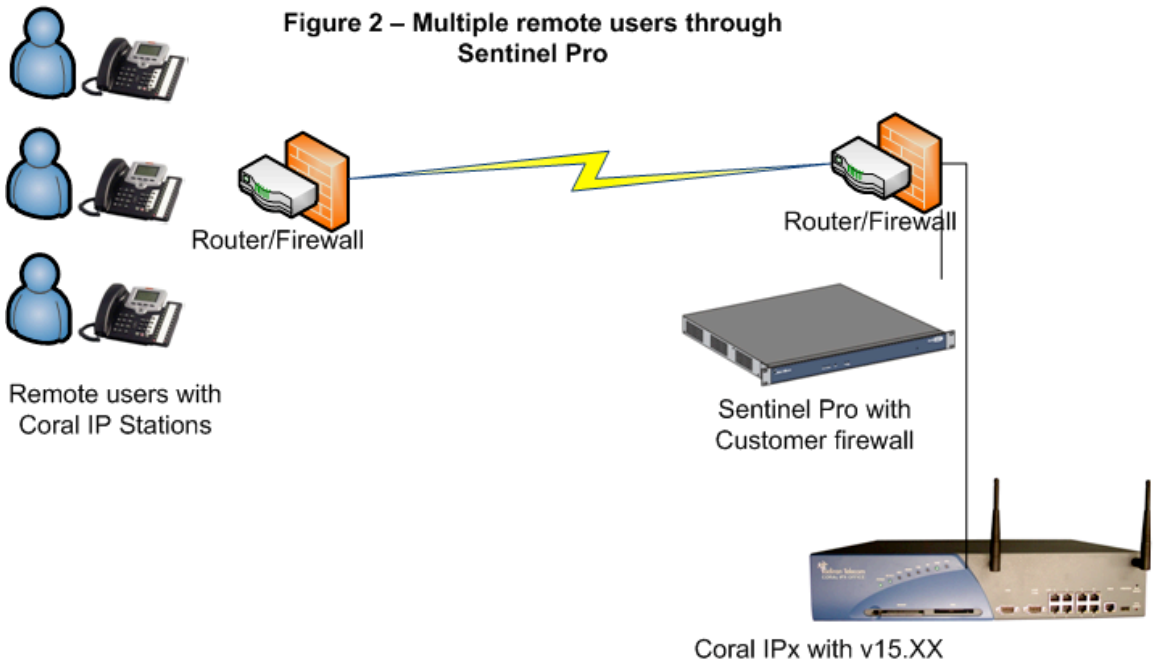
Also the local and remote routers can forward ports in their firewall. The routers at both ends will have to be allowed to forward ports 2427 (for MGCP), 5060 (for SIP), 16400 through 16992 at one end to the PUGW of the Coral and the other end to the user's IP telephone.

Security and connectivity without VPN Software

The Sentinel Pro allows connectivity without the need for VPN software or compliant routers. A Sentinel Pro will connect users in the following configurations:

1. A single user is behind a firewall or router that does not have port forwarding of ports (2427, 5060 and 16400 through 16992).
2. A single public IP address at a remote location with a firewall has more than one IP station behind it.

Figure 2 – Multiple remote users through Sentinel Pro



In these cases, the Sentinel Pro serves two functions. First the Sentinel Pro allows remote IP telephones to authenticate and connect to the Call Agent. Secondly, the Sentinel Pro converts the remote IP and port address combination to a unique IP address. This allows telephone conversations to take place seamlessly without having to sacrifice network security by opening up ports in the firewall.

The Sentinel Pro comes in four different sizes, depending on the number of simultaneous conversations (10, 25, 75, 150) that are required.

Summary

Companies are grappling with data security issues. Do we use unsecured IP devices that use open ports (i.e., port 80 used by the Internet) and risk security or toll fraud? Do we open ports or spend money on expensive data equipment at each office?

The Sentinel Pro allows companies to deploy a single Internet appliance to connect remote users with a minimum of security issues and programming.