



Security Levels White Paper

Abstract:

This paper presents several challenges of VoIP network security and different solutions.

The absence of adequate security in VoIP networks may present substantial threats for enterprise businesses.

The information contained in this document is proprietary and is subject to all relevant copyright, patent and other laws protecting intellectual property, as well as any specific agreement protecting TADIRAN TELECOM® LTD.'s (herein referred to as the "Manufacturer") rights in the aforesaid information. Neither this document nor the information contained herein may be published, reproduced or disclosed to third parties, in whole or in part, without the express, prior, written permission of the Manufacturer. In addition, any use of this document or the information contained herein for any purposes other than those for which it was disclosed is strictly forbidden.

The Manufacturer reserves the right, without prior notice or liability, to make changes in equipment design or specifications.

Information supplied by the Manufacturer is believed to be accurate and reliable. However, no responsibility is assumed by the Manufacturer for the use thereof nor for the rights of third parties which may be affected in any way by the use thereof.

Any representation(s) in this document concerning performance of the Manufacturer's product(s) are for informational purposes only and are not warranties of future performance, either express or implied. The Manufacturer's standard limited warranty, stated in its sales contract or order confirmation form, is the only warranty offered by the Manufacturer in relation thereto.

This document may contain flaws, omissions or typesetting errors; no warranty is granted nor liability assumed in relation thereto unless specifically undertaken in the Manufacturer's sales contract or order confirmation. Information contained herein is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify the Manufacturer. All specifications are subject to change without prior notice.

© Copyright by TADIRAN TELECOM® LTD., 2008.
All rights reserved worldwide.

The Coral is protected by U.S. Patents 6,594,255; 6,598,098; 6,608,895; 6,615,404

All trademarks contained herein are the property of their respective holders.

Table of Contents

| | | |
|-------|---|---|
| 1 | The Challenges | 4 |
| 2 | Security Threats..... | 5 |
| 3 | Sea Softswitch Security Levels | 5 |
| 3.1 | Security Plug | 5 |
| 3.2 | Operating System Level – Linux..... | 5 |
| 3.2.1 | SSH Security Layers..... | 5 |
| 3.2.2 | Transport Layer | 6 |
| 3.2.3 | Authentication | 6 |
| 3.3 | Sea Softswitch Hardening (Linux Server based)..... | 6 |
| 3.3.1 | Disabling Unnecessary Services..... | 7 |
| 3.3.2 | Remote Access and SSH Basic Settings | 7 |
| 3.3.3 | User ID | 7 |
| 3.3.4 | System Logging and Passwords | 7 |
| 3.4 | Centralized Administration | 8 |
| 3.5 | Secured replication process for Redundancy and Fault Tolerance..... | 8 |
| 3.6 | File Transfer Mechanism..... | 9 |
| 3.7 | Endpoint Terminal Encryption | 9 |
| 3.8 | Sentinel Pro – Session Border Controller..... | 9 |

1 The Challenges

Enterprises invest much effort and resources in building up their innovative next-generation networks. However, with increasing security threats, enterprises have to face the substantial challenge of how to protect their businesses and ensure continuity of communication.

Multiple methods can be used to protect your VoIP network. These methods can be categorized into two main concepts:

1. Prevention – to control your network, and deny the accessibility of intruders and unauthorized users to your network by using Firewalls, Network Access Control (NAC), and Session Border Controllers
2. Detection – to detect the intruders and the hostile source

Figure 1 presents multiple modules and the main required functionalities to protect your VoIP networks.

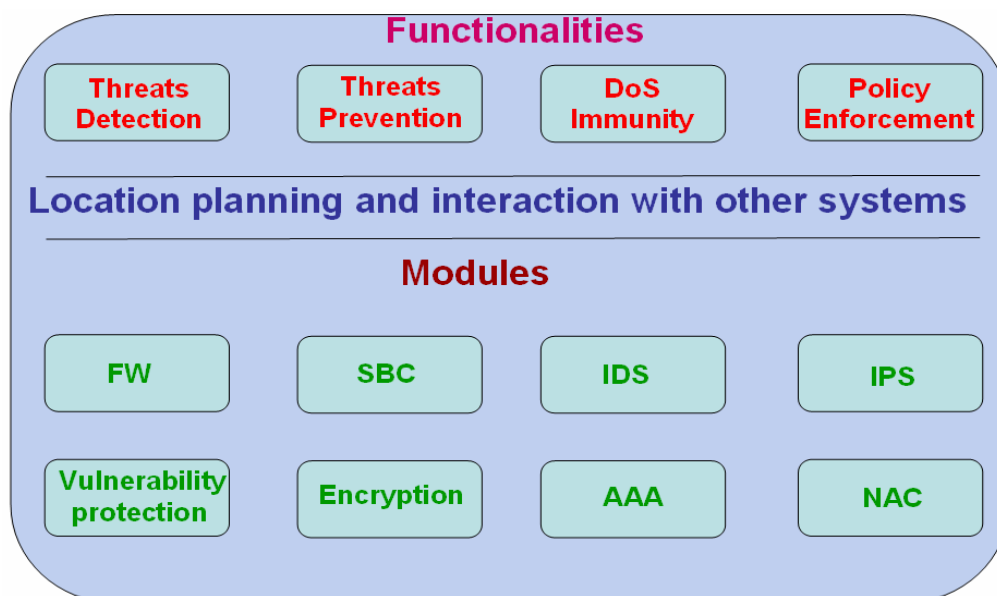


Figure 1

A firewall (FW) is widely used in VoIP networks as part of a security policy designed to safeguard the privacy of the enterprise network. Firewalls provide a single point of administration and control, allowing administrators to police and filter traffic that keeps unauthorized users, such as hackers or intruders, from breaking into the protected network.

One of the challenges of operating VoIP-based solutions behind a FW is the fact that RTP ports are dynamically allocated. In order to allow authorized traffic to penetrate firewalls, multiple ports need to be opened at the expense of security.

The typical, non-application aware firewall cannot handle VoIP traffic and must work in conjunction with another sophisticated component: The Session Border Controller.

However, there are already application-aware firewalls that were especially designed to work within the NGN environment. These firewalls can implement a Deep Packet Inspection (DPI) using VoIP stacks such as SIP, MGCP, SDP, RTP and RTCP.

2 Security Threats

Due to its wide deployment, a VoIP network can be exposed to a wide range of security threats and attacks.

VoIP may be deployed in relatively safe environments where the network equipment is trustworthy and the physical security is implemented sufficiently, or in potentially hostile Internet environments.

An Internet environment can be considered hostile for a number of reasons; mainly because attacks are not traceable.

Two types of possible threats exist:

1. External threats – attacks launched by someone not participating in the message flow during a VoIP-based call
2. Internal threats – these are much more complex because they are usually launched by a VoIP call participant.

There are several levels of threats that may interrupt the traffic and cause damages to the communication network:

1. Denial-of-service (DoS) attacks – prevention of getting services by flooding the Softswitch with multiple packets
2. Unauthorized interception of voice packets or of the Real-Time Transport Protocol (RTP) media stream, and decoding of signaling messages
3. Packet spoofing: Impersonation of a legitimate user sending data

3 Sea Softswitch Security Levels

3.1 Security Plug

A dedicated plug with a license key that holds the number of purchased Sea Softswitch licenses must be plugged into the USB connector of a Sea Softswitch server before the application can run. (If the plug is missing, a limited trial version will run instead and expire after two weeks.)

This plug prevents unauthorized personal from using the system.

3.2 Operating System Level – Linux

3.2.1 SSH Security Layers

For remote accessibility Tadiran utilizes the Secure Shell (SSH) to provide encrypted Telnet-like access.

The SSH protocol allows any client and server programs built to the protocol's specifications to communicate securely and be used interchangeably. Combined with the OpenSSL encryption libraries, OpenSSH provides a full-range of security capabilities.

3.2.2 Transport Layer

Once a client contacts the Sea server using the SSH protocol, several important points are negotiated so that the two systems can correctly construct the transport layer:

- Key exchange
- The public key algorithm to be used
- The symmetric encryption algorithm to be used
- The message authentication algorithm to be used
- The hash algorithm to be used

During the key exchange, the Sea Softswitch server identifies itself to the client with a host key. Then, in subsequent connections, the server's host key can be checked with a saved version on the client, providing confidence that the client is indeed communicating with the intended server.

3.2.3 Authentication

Once the transport layer has constructed a secure tunnel to pass information between the two systems, the Sea Softswitch server tells the client the different authentication methods supported, such as using a private key-encoded signature or typing a password. The client then tries to authenticate itself to the server using any of the supported methods.

The server decides which encryption methods it will support based on its security model, and the client chooses the order of the authentication methods from among the available options.

Note: Thanks to the secure nature of the SSH transport layer, even seemingly insecure authentication methods, such as host-based authentication, are safe to use.

3.3 Sea Softswitch Hardening (Linux Server based)

When implementing system security, Tadiran complies with several fundamental concepts for keeping the Sea Softswitch system secure. Patch management (keeping software up-to-date) and system hardening (disabling unnecessary services) are vital, as are overall security policies, change management, and log file audits.

The list presented below does not remove all risks, but reduces the overall probability of risks.

| No. | Security Elements |
|-----|---|
| 1. | <p>3.3.1 Disabling Unnecessary Services</p> <p>Hardening the Sea Softswitch server by removing unnecessary services enhances security and improves overall system performance. Furthermore, as part of Tadiran's security policy, Samba is not installed.</p> |
| 2. | <p>3.3.2 Remote Access and SSH Basic Settings</p> <p>SSH is a client-server based tool used for remote administration of servers via a terminal console. With SSH, authorized Sea Softswitch users can log in to a remote machine and run commands, transfer files using SFTP or SCP, and more.</p> <p>As Telnet is not recommended for remote access, and in order to reduce vulnerabilities, Tadiran uses Secure Shell (SSH), which provides encrypted Telnet-like access and is considered a secure alternative to Telnet. SSH encryption is based on public-key/basic key cryptography.</p> <p>Port scanners commonly attack TCP port 22, which is the port SSH uses by default. Running SSH on an alternate port is a basic but highly efficient means against such attacks.</p> <p>Furthermore, it is recommended to use the firewall's IP-Tables to limit access by IP address or host/domain name.</p> |
| 3. | <p>3.3.3 User ID</p> <p>To leverage the system security, use another username than "root".</p> |
| 4. | <p>3.3.4 System Logging and Passwords</p> <p>The Linux-based Sea Softswitch server includes a logging mechanism, which is important for troubleshooting system failures, network problems, and security incidents.</p> <p>Logging on to the server is controlled by a Syslog daemon. The log files are owned only by the root user, therefore they are not available to the casual user.</p> <p>Note: All accounts have passwords that meet the password standards in the security program and consist of at least 8 characters.</p> |

3.4 Centralized Administration

In order to be access the Sea Softswitch centralized management system (Web Admin) and remotely manage and provision the system, a user name and password have to be used.

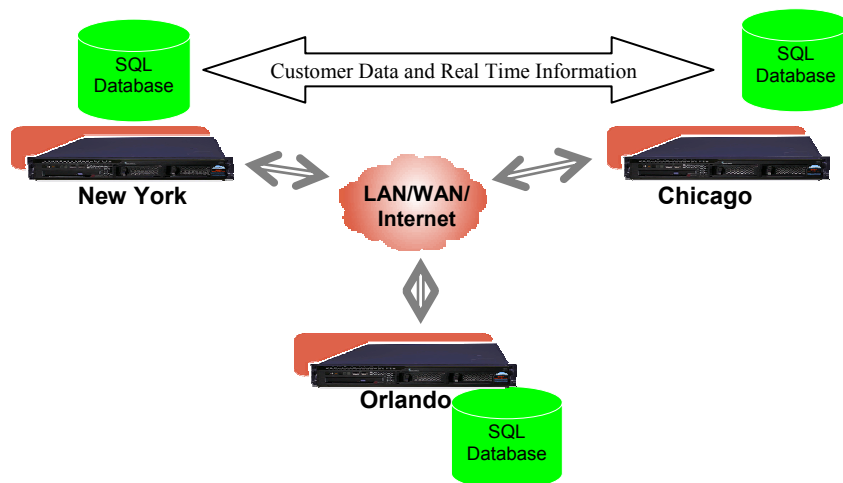
This authentication mechanism provides another level of security for preventing unauthorized personal from accessing the Sea Softswitch and the associated Wave Gateways.

The centralized management system can be accessed from Windows-based PC. Windows Vista (or XP) has its own security level, which should be used. It requires administrators to log in to the PC and identify themselves before they can use the PC. Enterprises are also recommended to use NAC (Network Access Control) to ensure user access integrity.

All the information between the Web Admin and the Sea Softswitch is transmitted using the Hypertext Transfer Protocol over Secure Socket Layer or HTTPS (secure HTTP connection).

3.5 Secured replication process for Redundancy and Fault Tolerance

Each server in a Sea Softswitch deployment accesses the same database. In duplicated or multiple Sea Softswitch server environments, all customer information and events in the Sea Softswitch are maintained inside each server, including events and configuration changes, which are copied simultaneously to all servers.



This sharing of information ensures that unlike cluster storage systems, which are typically made up of network-connected storage with a collection of managed physical disks that store static information, all Sea Softswitch servers share the dynamic information or event states of all endpoints, gateways and users in an enterprise network along with database information.

During the replication process, vital information is transferred between Sea Softswitch servers.

The replication mechanism which is based on GigaSpaces, provides role-based security, allowing administrators to define fine-grained permissions. GigaSpaces also provide, as an option, encryption of the transferred-data.

3.6 File Transfer Mechanism

The Web Admin utilizes SFTP. Like FTP, SFTP is an interactive file transfer protocol, but it performs all operations over an encrypted transport layer. It also uses public key authentication and compression methods.

3.7 Endpoint Terminal Encryption

Tadiran's IP phones provide a high level of security by supporting the Triple DES encryption.

Triple DES offers much more security than the regular DES algorithm. It encrypts the data using a regular DES key, but then decrypts it with another key and re-encrypts the decrypted output using the first key. With each key consisting of 56 bits, Triple DES provides effective protection against brute-force and meet-in-the-middle attacks.

3.8 Sentinel Pro – Session Border Controller

The Sentinel Pro is a Session Border Control (SBC) unit that enables the connection of remote IP phones located behind NAT (Network Address Translation) servers or firewalls. 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 Sentinel Pro 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 transverse the server
- Establishes local RTP sessions between remote MGCP IP endpoints located behind the same NAT server, thereby freeing up Sentinel RTP resources
- Leverages the traffic capacity toward the Sea Softswitch ensures DoS immunity and services continuity (Traffic Mitigation)
- Signaling Integrity – implementing DPI, the Sentinel Pro ensures message integrity at the SIP, MGCP, SDP, IP, and UDP layers. It verifies that the message received is the same as the message that was sent. In case abnormal messages are received, these messages will be dropped out and therefore not overload the Sea Softswitch.

Firewalls do not allow direct connection from the outside world to the internal LAN, as signaling and media traffic must first travel through the firewall.

The Sentinel Pro acts as a transmission point, enabling all signaling and media traffic to be routed to and from the remote IP endpoints.

NAT devices assign a unique IP socket to every RTP session upon call setup. The Sea Softswitch (or any other call agent or registrar) is unable to set up a session without knowing which port the NAT will assign.

To address this, the Sentinel Pro acts as a meeting point. The IP endpoints direct their RTP streams towards the Sentinel Pro, which detects the source IP socket, adjusting the destination of the RTP streams it transmits accordingly.

The Sea Softswitch (as any call agent or registrar) assigns specific ports for the handling of VoIP signaling data (2427 or 2727 for MGCP, 5060 for SIP). The IP sockets of incoming sessions have to be adjusted to contain the relevant port number.

The Sentinel Pro acts like multiple virtual IP endpoints that receive the calls, redefine the incoming IP sockets, and route them to the Sea Softswitch unit through the relevant signaling port.