BLOX

Quick Installation Guide

Copy Right

Proprietary Rights

Disclaimer

About this manual

This manual describes the Blox product application and explains how to work and use it major features. It serves as a means to describe the user interface and how to use it to accomplish common tasks.

Document Conventions

In this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. Additionally, this document has different strategies to draw User attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning.

Icon	Purpose
	Note
	Tip/Best Practice
	Important
	Caution
	Warning

- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color blue with underline is used to indicate cross-references and hyperlinks.
- Numbered Paragraphs - Numbered paragraphs are used to indicate tasks that need to be carried out. Text in paragraphs without numbering represents ordinary information.
- The Courier font indicates a command sequence, file type, URL, Folder/File name e.g. www.blox.org

Support Information: Every effort has been made to ensure the accuracy of the document. If you have comments, questions, or ideas regarding the document contact online support via Skype: blox.support

Table of Contents

1. Overview

Blox is the industry's first open source software-based Session Border Controller that delivers the scalability with the advanced features and functionality. The Blox features media Transcoding, security technology and policy based routing.

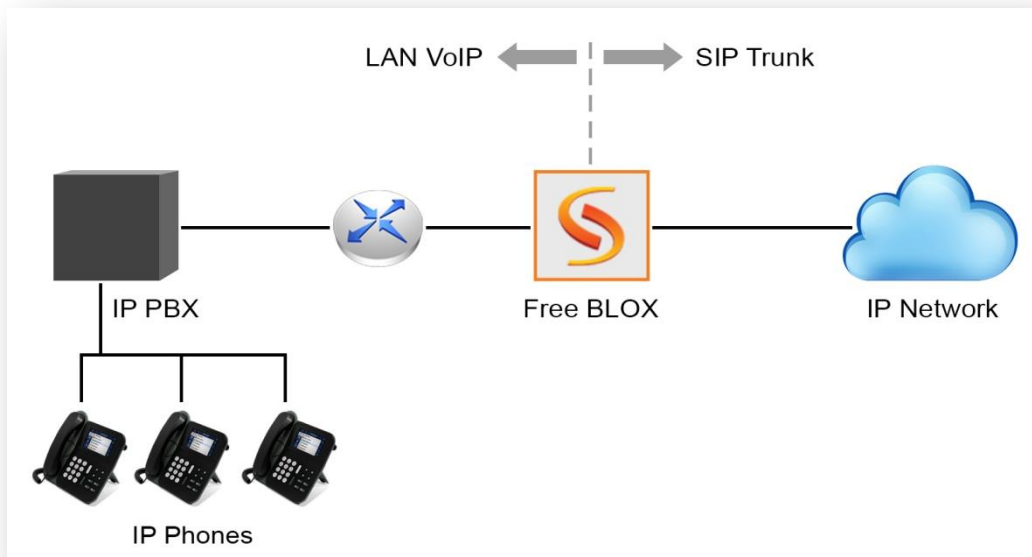Below diagram explains the typical implementation and application of Blox.

Figure 1: Overview of Product

The Blox sit's at the edge of the network to provide control over the SIP traffic. Traditionally they were seen as just providing firewalling protection – the security – for SIP-based voice networks. E-SBC's do indeed provide the security, which is absolutely a critical function, but have evolved to serve as a crucial element in **enabling** SIP deployments.

See what you get with the Blox (Software Edition)

 Normalize the SIP signaling so that the IP-PBX at the customer site and the service provider's network are fully compatible. While SIP is a standard, each implementation can be slightly different, and the service providers may require a different level of authentication from the business. With the Blox in place, these requirements can be met.

Additionally, normalization of the SIP signaling allows service providers to support more IP-PBXs, or those IP-PBXs that are not yet certified by the ITSP. In this manner the ITSP can provide a wider

array of options for their customers and expand their business without the need for extensive interoperability certification with each IP-PBX.

Resolve NAT traversal issues to enable the adoption of SIP, SIP trunking and full Unified Communications by securely permitting SIP signaling and related media to traverse the firewall. Without this function, most companies will have one-way audio only.

Security through deep packet inspection (DPI): DPI is a powerful way to protect not just SIP traffic, but also the network. It is a form of computer network packet filtering that examines the data (or datagram) and UDP/TCP header part of a packet as it passes through a Blox. DPI can be effective against buffer overflow attacks, denial of service (DoS) attacks, sophisticated intrusions, and a small percentage of worms that fit within a single packet.

Control through authentication: Many service providers require authentication of the user with their network. Some IP-PBXs do not support this function. With the Blox in place the service provider's requirement can be met regardless of which IP-PBX is used.

Encryption: Encryption features are inherent in the SIP protocol and when used between two sites minimize any opportunity for unrelated parties to intercept the call. This offers maximum privacy even over the public Internet.

Intrusion Detection/Prevention: The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) in Blox's Enhanced Security software module enables the Blox to detect DoS attacks based on SIP, and to block malicious SIP signaling packets designed to attack certain SIP phones, servers or other devices on the enterprise LAN. This secures the enterprise network as the Blox handles the attacks while the servers and other SIP devices in the network can still be used.

2. Deployment Considerations

Blox is deployed in the following different scenarios

Scenario 1

The Blox has been made to control VoIP signaling and media streams and it's responsible for setting up, conducting and tearing down calls. So, it's recommended to deploy the Blox along with the PBX as given in the following scenarios based on what is applicable in the user's setup.

Figure 2: Scenario 1

Scenario 2 -Single-box Blox Deployments

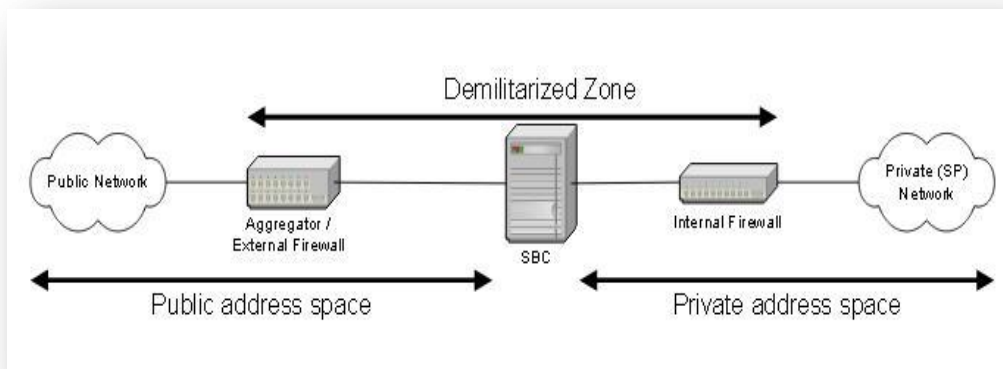Single-box Blox deployed in the DMZs of VoIP-enabled service provider (SP) networks.

Figure 3: Scenario 2

Scenario 3- Reduced Demilitarized Zone

In this scenario, the Blox is the only application-aware device in the DMZ. As such, when applications within the private network require IP traffic to traverse the DMZ, the Blox takes responsibility for ensuring that the other equipment within the DMZ allows that traffic through.
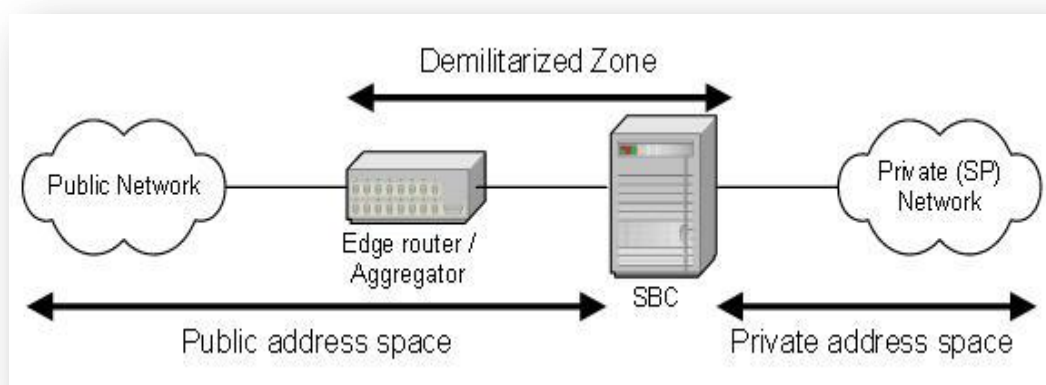
Figure 4: Scenario 3

Scenario 4- Dual box Blox Deployments

In this scenario, all VoIP signaling traffic received from the public network is allowed through the DMZ and routed to Blox-SIG.
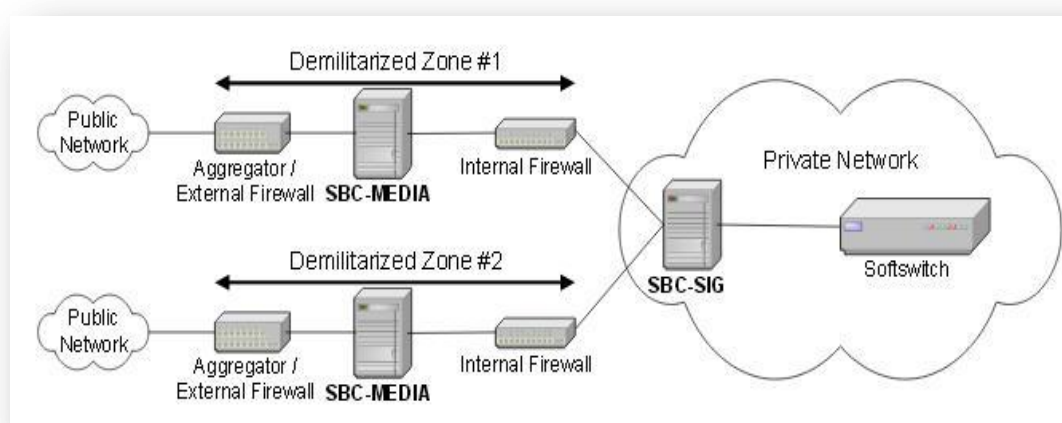

Figure 5: Scenario 4

3. Minimum Hardware Requirements

Minimum Hardware Requirements (Up to 90 concurrent calls)

- Dual core Intel processor with 64 bit architecture

- 2GB of RAM

- 2 Network Interfaces (10/100/1000 Mbps)

- 80GB hard disk space

4. Software Installation Steps (ISO Image)

1. Download the BLOX ISO file from here: http://blox.org/downloads & burn it to the DVD. The ISO image consists of Linux operating system and BLOX SBC.

2. If booting from the installation media succeeds, you should see the ISO image installer welcome screen. Press ENTER to continue the installation. The installer will subsequently be loaded; this can take a few minutes.

3. The installer will ask for the primary disk or disk array. The primary disk will hold the ISO image operating system and the database.

The primary disk can have a size between 7GB and 8GB. If you wish to use a larger disk array for data storage, configure it as a secondary disk.

4.1 ISO Installation

To complete the ISO installation, follow these steps:

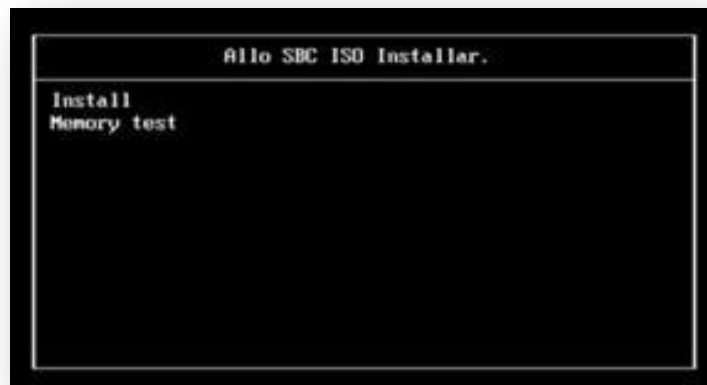1. Boot the server with the ISO Image, A screen similar to the one shown below appears.

Figure 6: ISO Installer

2. To start the installation process, choose the first option Install. This process takes a few minutes to complete.

3. Select the language, Key board selection & time zone, would you like to continue to use during the installation process.

4. Root Password: you must type it twice to ensure you know it and do not make a typing mistake.
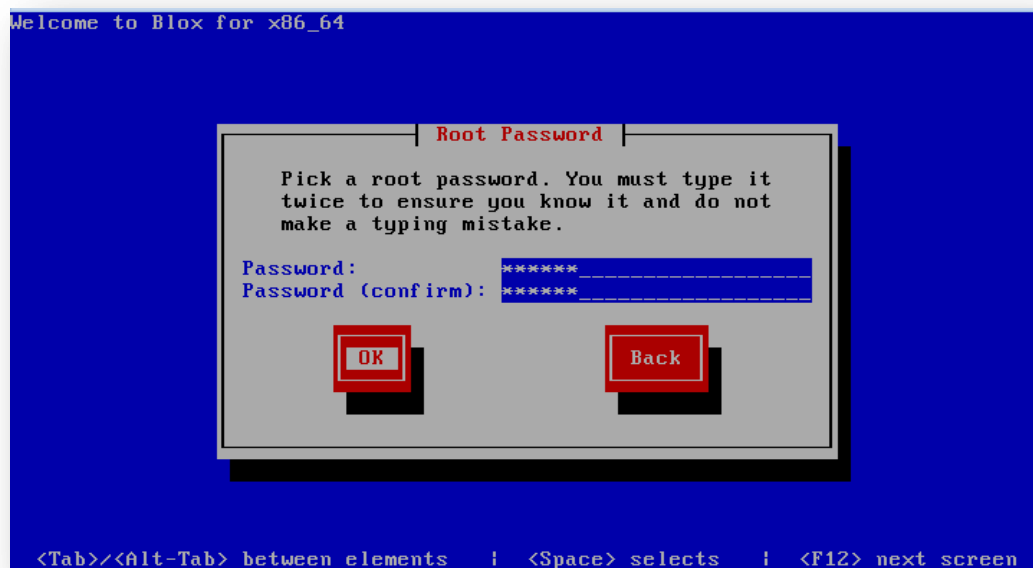
Figure 7: Root Password

5. Installation requires partitioning of your hard drive and the default layout is suitable for most users. Select what space to use and which drivers to use as the install target.
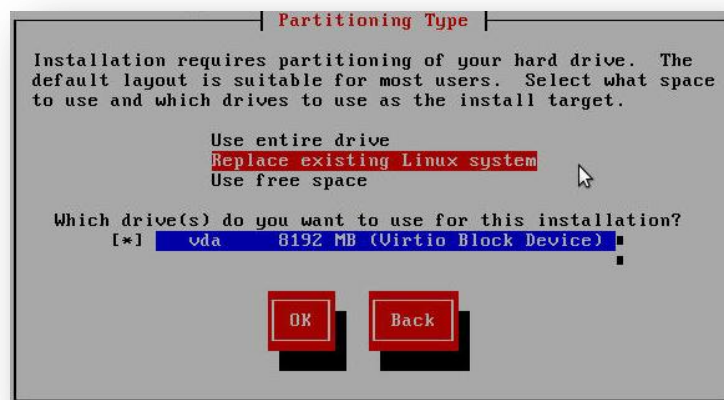

Figure 8: Partitioning Type

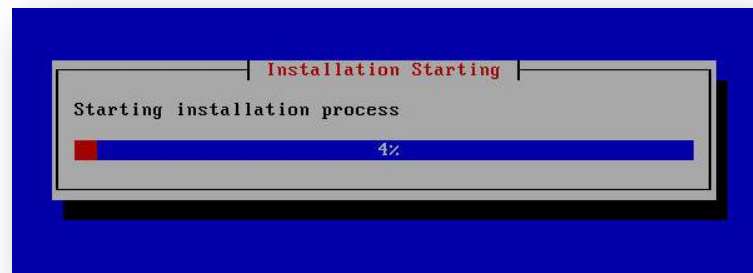6. After select the partitioning type, click ok to start the installation process.

Figure 9: Installation Starting

7. During the package installation, installing Kernel-headers-2.6.32-431.28.5.e16.x86_64 (2MB) Header files for the Linux Kernel for use by glibc.

Figure 10: Package Installation

8. Please wait while the installation starting process will takes a few minutes to complete.

9. Finally the installer will reboot the system. When instructed, remove the DVD used for the installation. After rebooting, the machine will show the IP address it uses.

Figure 11: Apply Firewall Rules

10. System will get default IP address via DHCP or it can be manually configured. To configure
    login and run the following command

$ setup

This leads to the selection of network interface selection through user interface (Follow step11).If
you want to set the IP address through CLI, use the following:

`$ ifconfig eth0 <ip address> Netmask<x.x.x.x>`

For Eg: $ ifconfig eth0 192.168.1.10 netmask 255.255.255.0

11. **Select network configuration**

When the machine starts up after power on, it automatically uses DHCP to obtain its network
configuration information. A DHCP server delivers an IP address as well as other configuration
settings to the machine.

Once select the network configuration, click Run Tool to run the configuration.

Figure 12: Network Configuration

12. **Select device configuration**

A common device configuration comprises user-specific service and feature attributes. Ensure that each device is associated with a common device configuration for user-oriented information.

Figure 13: Device Configuration

13. **Select the interface**

You can configure specific properties on your Ethernet interface to ensure optimal performance of your network.

Figure 14: Selection of Device

14. Configure and save the network and run the following command.
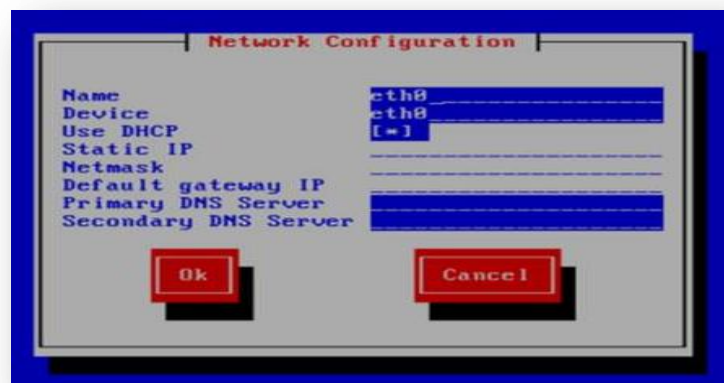
```
$ Service network restart
```


Figure 15: Network Configuration

15. To find the IP address of the system run the following command

```
$ ifconfig -a
```

Figure 16: Login page

16. Blox Installation is completed.

5. FreeBlox Installation (User Interface)

FreeBlox is the GUI designed for Blox SBC & user can configure the features and the SBC administration.

5.1 Prerequisites

1. Download and Install Blox in 64 bit Machine that meets the minimum requirements indicated here: http://blox.org/downloads

2. Configure the Network setup for Blox (follow instruction as per Quick Installation guide step: 10)

You can avail the FreeBlox GUI for easier configuration of the SBC. Please contact us enquiry@blox.org

Any Technical assistance required, Kindly contact the support at support@blox.org or SKYPE: blox.support

THANK YOU!

Thank You