

WHITE PAPER

---

# KLIR SECURITY OVERVIEW

## for Customer Network Security Officers

Frank Fulton  
April 5, 2006

---

Klir Technologies provides an on-demand, hosted solution for monitoring and analysis of IT infrastructure, including network traffic, servers and applications. The Klir Appliance (a device that resides on the monitored network) securely collects and transports data from a customer's network devices to the Klir Data Center, where it is analyzed and stored in the Klir On-Demand Services Platform (Klir Platform). The data is made available to users anytime and anywhere through Klir Analytics, a hosted web application that provides drill-down analytics, role-specific dashboards, customized reporting and sophisticated alerting.

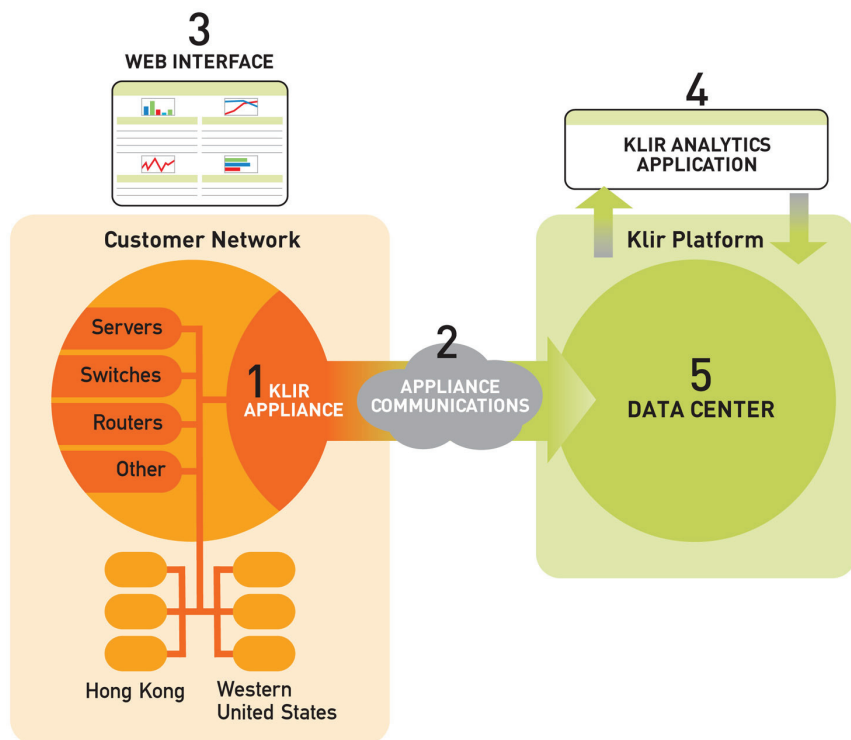
## Introduction

Klir Technologies provides an on-demand, hosted solution for monitoring, managing, and analysis of IT infrastructure, including network traffic, servers and applications. The Klir Appliance, a device that resides on the customer's network, securely collects and transports data from network devices to the Klir Data Center, where it is analyzed and stored in the Klir On-Demand Services Platform (Klir Platform). Users can access this data anytime, anywhere via Klir Analytics, a hosted Web application that provides drill-down analytics, role-specific dashboards, customized reporting and sophisticated alerting.

This document describes the security components of Klir's on-demand architecture, including the customer's network, the Klir Data Center and communication between the two.

The document is divided into the following sections:

- 1 Klir Appliance Security
- 2 Klir Appliance Communications Security
- 3 Web Interface Security
- 4 Klir Platform Security
- 5 Klir Data Center Security



# 1

## Klir Appliance Security

The Klir Appliance includes the following security measures and components:

- **Automatic updates and monitoring.** Klir manages and continually monitors the appliance to ensure it is running correctly and is up-to-date.
- **Hardened operating systems.** The appliance servers run Debian Linux with a hardened gsecurity-based Linux kernel (version 2.6).
- **Restricted configuration.** Any unnecessary protocols, processes, users and network connections have been removed.
- **No command or control capabilities.** The Klir Appliance collects read-only performance data and has no command or control capabilities over any devices on the customer network.
- **Data collection on specified devices only.** The Klir Appliance collects data only on devices specified by the customer.
- **Simple Network Management Protocol (SNMP) data collection.** The Klir Appliance collects read-only data via SNMP version 1 or 2c. SNMP-compliant devices store data about themselves in management information bases (MIBs). This information is served to SNMP requestors that supply the correct community string.
- **Flow data collection.** The Klir Appliance collects flow data only from network devices configured to send flow data to the appliance. The Klir Appliance is not in line with other network devices and therefore cannot intercept data.
- **Packet header analysis.** Klir receives only packet header information. No packet content is accessed, or can be accessed, by the appliance.
- **Access managed through access control lists (ACLs).** Access to each monitored device can be restricted through ACLs.

The Klir Appliance is available in two configurations, standard and high-availability. The high-availability configuration comprises two appliances in an active/passive configuration. If the primary fails for any reason, the passive becomes active and takes over immediately.

## 2

### Klir Appliance Communications Security

The Klir Appliance communicates over dedicated ports by using industry-standard protocols to ensure secure data transport. Appliance communications are secured as follows:

- **From the Klir Appliance to the Klir Data Center.** Communications are secured through Secure Sockets Layer (SSL) version 3 or Transport Layer Security (TLS) version 1 by means of the OpenSSL library. Authentication is performed bi-directionally through RSA 2048-bit X.509 certificates and data is encrypted using 256-bit Advanced Encryption Standard (AES) encryption. All communication (except communication related to updates) is initiated by the Klir Appliance.
- **From the Klir Data Center to the Klir Appliance.** The only communications initiated by the Klir Data Center are automatic updates. Authentication is performed through pre-shared 2048-bit Digital Signature Algorithm (DSA) keys, and data is encrypted using secure shell (SSH) encryption.

## 3

### Web Interface Security

Users log in to the Klir Analytics application through a secure Web interface. The connection between the browser and the Web server is secured through industry-standard procedures and protocols, as follows:

- **1024-bit authentication and SSL v3.0 or TLS v1.0.** The level of encryption is negotiated with the client browser. Klir Analytics supports up to 256-bit encryption.
- **User ID and password.** Passwords are stored through secure hash algorithm version 1 (SHA-1) so they cannot be stolen as plain text, even with direct database access.

# 4

## Klir Platform Security

The Klir Platform is secured through a combination of internal policies and network security measures.

Internal policies that safeguard the hosted application include the following:

- **Strict rights management.** Rights are restricted to only necessary services and qualified personnel.
- **Limited physical access.** The application servers are housed in locked cages accessible by card keys.
- **100% failover/redundancy.** Every layer in the stack provides complete failover and redundancy.
- **Database backups and archives.** All data is backed up and archived regularly and securely.

Network security measures include the following:

- **Commercial-grade firewalls.** Top-tier, commercial-grade firewalls with strict policies secure and maintain data and applications.
- **Network address translation (NAT).** NAT ensures internal IP addresses are hidden and not routable from the outside.
- **IP masquerading (IPMASQ).** IPMASQ gives the appearance (to external observers) that all data is coming from and going to the same IP address.

# 5

## Klir Data Center Security

The Klir Data Center is located inside a tier 1 telecommunications facility, which is secured as follows:

- **Solid construction.** The Klir Data Center can withstand almost any type of disaster.
- **Highly available and reliable network connectivity.** Redundancy at every level and self-healing devices ensure high availability.
- **Continuous security.** Professional security personnel are present 24x7.
- **Restricted access.** Use of card keys, keypads and biometrics, all under video surveillance, ensures that access is restricted to authorized personnel.
- **Redundant backups.** Backups are duplicated and stored at a remote site.
- **Fire suppression.** Zoned smoke detection and a fire suppression system protect against fire damage.
- **Redundant power.** Uninterruptible power supply (UPS) batteries and diesel-powered generators insure against power failure.